THE FINANCIAL IMPACT OF BREACHED PROTECTED HEALTH INFORMATION

A Business Case for Enhanced PHI Security

ANSI
American National Standards Institute

SHARED ASSESSMENTS

INTERNET SECURITY ALLIANCE

TABLE OF CONTENTS

PROJECT TEAM

Acknowledgments

The following professionals are acknowledged for their contributions to the development of this report through participation in project meetings and teleconferences.

The report was developed based on their collective inputs, following a consensus process, and does not necessarily reflect the views of the companies and organizations listed.

ActiveHealth Management	Manomohan Kalathil
Aeritae Consulting Group, Ltd.	Rob Ramer
Affinion Security Center	Christine El Eris*
Alvarez & Marsal	Mandar Rege
American Health Information Management Association	Harry Rhodes
American National Standards Institute	Jim McCabe, Liz Neiman, Sally Seitz
Androscoggin Home Care & Hospice	Julie Porter
AWARE Software, Inc.	Dr. James Zaiss
B System Compliant, LLC	Rustom Bhopti
Bayhealth Medical Center	Bonnie R. Millman
BKD LLP	Matthew Lathrom
Blue Cross Blue Shield of Michigan	Dawn Geisert
Bluewater International	Dr. Gary R. Gordon*
Booz Allen Hamilton Inc.	Debbie Wolf,* Ilene Yarnoff
Catholic Health Initiatives	Carrie Harding
The Center for Identity Management and Information Protection at Utica College	Dr. Don Rebovich,* Ingrid Norris, Barb Stack
Church Pension Group Services Corp.	Stephen Tihor
Clearwater Compliance LLC	Bob Chaput, Mary Chaput, Eric Lombardo, Jon Stone
CyberRisk Partners	Alfred Bartkiewicz
Deluxe Corporation	Linnea Solem*
Direct Computer Resources, Inc.	Ed Stull*
DriveSavers Data Recovery, Inc.	Lynda Martel*
eLCHEMY, Inc.	Erin E. Kenneally

Europ Assistance USA	Michael Billings, Vladimir Poletaev
Evantix	James Christiansen*
Foley & Lardner LLP	Peter McLaughlin, Andrew B. Serwin*
FS-ISAC	Eric Guerrino
George Washington University	Patricia MacTaggart
HCA, Inc.	David Vulcano
Health Market Science	Michael Nelson
Henry Ford Health System	Meredith Phillips
IBM Corporation	Jon Bogen
ID Experts	Christine Arevalo,* Bob Gregg, Rick Kam,* Doug Pollack
Identity Theft Resource Center	Linda Foley
Independent Consultant	Vivek Desai
Independent Consultant	Susan A. Miller, J.D.
Independent Consultant	Jane Schweiker
Independent Consultant	David Walling
Independent Consultant	Richard E. Wolfe
Information Law Partners	Regan Adams
Internet Security Alliance	Larry Clinton,* Joshua Magri, Stephanie Schaffer
Kraft Foods Global	Abhishek Agarwal
LMI	Roxanne Everetts, Virginia Stouffer
McKesson Corporation	Louise Smith, John B. Sapp Jr.
MCM Solutions for Better Health	Amy Gasbarro
Meditology Services	Cliff Baker, Bethany Page
Middlegate Med	Dr. Sean Scorvo
MPV	Nicole Miller
North American Security Products Organization	Ann Whitehead
North Carolina Healthcare Information & Communications Alliance Inc.	Holt Anderson
N-Tegrity Solutions Group	Mark Cone
OlenderFeldman LLP	Aaron Messing, Joseph S. Pecora, Jr.
Orchestrate Healthcare	George J. Gides, Jr.
Patterson Companies, Inc.	Adam Stone
Phillips Nizer LLP	Thomas Jackson
Ponemon Institute	Dr. Larry Ponemon*
Powers Pyles Sutter & Verville PC	James C. Pyles*
Robert Pinheiro Consulting LLC	Bob Pinheiro
Sallie Mae	Michael Castagna
The Santa Fe Group	Catherine Allen,* Robin Slade, Kelly Wagner
Science Applications International Corporation	Marsha Young
Sentar Inc.	Deborah Williams
Shared Health	Abraham Gilbert
Sky Catcher	Wendy Richards
Stay Well Health Management	Christine Sublett

Summit Security Group, LLC	Dan Briley
Swarmology Inc	Malcolm Bohm
Symantec	Axel Wirth
Terra Verde Services	Don Turnblade
Triad Biometrics LLC	Scott Coby
Trinity Mother Frances Hospitals and Clinics	Patrick Leech
Tunitas Group	Bill Pankey
University of California	Grace Crickette
University of Kansas	Jane M. Rosenthal
University of Texas Center for Identity	Dr. Suzanne Barber
Veriphyr	Nicole Borner
Wells Fargo Insurance Services, Inc.	Tim McClung
Wentworth-Douglass Hospital	Peter Lincoln
West Virginia Dept. of Health & Human Resources	Ellen Cannon
The White Stone Group, Inc.	Gretchen S. Johnson
Zafesoft	Sandeep Tiwari*

*Subcommittee co-chair

Thanks and acknowledgments are given for the support and participation of all the organizations that supplied experts to this initiative. Without the contributions of these individuals and their collective expertise, particularly those that chaired the various subcommittees and that participated actively, this final deliverable would not have been possible.

- Special acknowledgment and appreciation is given to Rick Kam of ID Experts for being the project chairman and co-chair of the Finale subcommittee, and to Ed Stull of Direct Computer Resources, Inc., for co-chairing the Finale subcommittee. Their leadership and dedication in helping to shape the initiative, lead its proceedings, and build consensus for the final deliverable were instrumental in reaching a successful outcome.

- Special thanks also go to Mary Chaput of Clearwater Compliance LLC for many hours spent editing the document and synthesizing the various inputs into a coherent report.

- Appreciation is given to the American National Standards Institute (ANSI), The Santa Fe Group, and the Internet Security Alliance (ISA) for the effective project management that kept this initiative on track and allowed for a successful delivery of the final publication in a timely manner, particularly from Jim McCabe, Liz Neiman, and Sally Seitz of ANSI; Catherine Allen, Robin Slade, and Kelly Wagner of The Santa Fe Group; and Larry Clinton, Joshua Magri, and Stephanie Schaffer of ISA.

- Special acknowledgment is given to Powers Pyles Sutter & Verville PC and the Consumer Electronics Association (CEA) for hosting project meetings.

- Special thanks are extended to Deluxe Corporation for printing the report.

- Appreciation is also extended to ID Experts and MacKenzie Marketing Group for their support on communications and outreach activities.

- Thank you to the following outside reviewers for their insightful comments on the draft report which contributed to the final version presented here:
  - Mary N. Chaney, Founder and CEO, MBS Information Security Consulting, LLC
  - James H. Dykstra, Principal, Edington, Peel & Associates
  - Dr. John Adams Fox, President and CEO, FFC Computer Services, Inc.
  - Mathieu Gorge, Founder and CEO, VigiTrust
  - Don Horn, Director of Information Security, CareFirst Blue Cross Blue Shield
  - Dr. Michael Kraten, President and co-founder, Enterprise Management Corporation
  - Michael Mahoney, President, Americas and Northern Europe, International SOS
  - Dr. John R. Powers, past Executive Director, President's Commission on Critical Infrastructure Protection
  - Randy V. Sabett, Counsel, ZwillGen, PLLC
  - Gail Scott, Washington diplomatic consultant, author, and advisor
  - Thomas J. Smedinghoff, Partner, Edwards Wildman Palmer LLP
  - Dr. Robert Wah, Chief Medical Officer, CSC
  - Christopher Steinbach, Chairman and CEO, The Newberry Group

- Thank you to Robert Gardner, New World Technology Partners, for leading the outside review effort and for providing the consolidated and insightful feedback to the project leadership.

- This initiative was made possible through the generous support of the following organizations: Clearwater Compliance LLC and DriveSavers Data Recovery, Inc. (premium sponsors); Affinion Security Center; Alvarez & Marsal; BKD, LLP; Booz Allen Hamilton; The Center for Identity Management and Information Protection at Utica College; Deluxe Corporation; Direct Computer Resources, Inc.; Europ Assistance USA; ID Experts; Terra Verde Services; and ZOHO ManageEngine (partner sponsors).

EXECUTIVE SUMMARY

Health privacy has long been perceived as the right of individuals and a necessity for effective, high quality health care. Individuals are willing to disclose the most intimate details about themselves to their doctors only with the trust that their health information will remain private and secure, whether it resides in a file at their doctor's office, on a hospital chart, or in a claims form at their insurance provider. Indeed, protecting health information privacy has been a core component of the minimum standards for the ethical practice of medicine for thousands of years.

As the health care industry moves to adopt electronic health records (EHRs), thereby creating multiple and more expansive databases in numerous locations, there is an increase in the number of people with access to protected health information (PHI), and many more opportunities for this information to be accidentally or intentionally disclosed, lost, or stolen. This new technological capability does not alter professional ethics, and indeed emboldens the resolve to protect the privacy and security of health information to preserve access to quality health care.

Daily headlines suggest that not all organizations entrusted with PHI protection are upholding their responsibility. Health information data breaches are increasing in number and in magnitude. Insufficiently trained staff are much to blame, but the fraudulent use or sale of PHI is also on the rise. Such breaches can cause significant harm, both to the individuals whose information was breached and to the organizations responsible for protecting it.

Regulations promulgated in the last few years provide incentives for an organization's "meaningful use" of EHRs, as well as increased enforcement and penalties for non-compliance with state and federal security regulations. Unfortunately, efforts to assure the confidentiality and integrity of PHI content have not kept pace. Individuals responsible for protecting the security of PHI face a number of challenges that may inhibit their ability to meet that responsibility, including legal and regulatory complexity, as well as lack of time, resources, and leadership commitment.

This report provides information that will enable organizations in the health care sector to build a strong business case for the benefits of investing in PHI protection and turning compliance with privacy and security laws to their market advantage. The report explores the reputational, financial, legal, operational, and clinical repercussions of a PHI breach on an organization, and offers a 5-step method – PHIve (PHI Value Estimator, pronounced "five") – for evaluating the "at risk" value of their PHI. This tool estimates the overall potential costs of a data breach to an organization, and provides a methodology for determining an appropriate level of investment to reduce the probability of a breach.

A comprehensive resource about the critical importance of safeguarding PHI, the report offers information about the stakeholders involved in the health care ecosystem; the evolution of laws, rules and regulations designed to protect PHI; the causes and increasing number of data breaches; the most common threats and vulnerabilities to the security of PHI; and safeguards and controls that organizations can put in place to mitigate the risk of a breach.

Organizations can head off the consequences of a PHI data breach by thoughtfully investing in enhancing their privacy and security programs.

The report also includes insights on current industry practices and attitudes in relation to protecting PHI, which emanated from a survey of individuals responsible for safeguarding this important health data.

Armed with the information contained in this report, organizations operating in the health care sector can head off the potentially devastating consequences of a PHI data breach by thoughtfully investing in enhancing their privacy and security programs at a level that reduces that probability or impact.

This report is organized as follows:

- Chapter One: An overview of how the health care ecosystem has expanded in recent years to include more organizations, all with the responsibility for the protection of PHI.
- Chapter Two: A comprehensive summary of how the laws and regulations that impact PHI protection have evolved since the enactment of HIPAA, the *Health Insurance Portability and Accountability Act of 1996*, including gaps and weaknesses in those laws.
- Chapter Three: A review of some recent PHI breaches – what happened and how – along with a discussion of the value of PHI.
- Chapter Four: A discussion of the more common threats now facing all organizations in the health care ecosystem and related vulnerabilities, including a case study of the repercussions of a PHI breach.
- Chapter Five: Highlights of the interaction and effectiveness of certain safeguards and controls related to policies, procedures, and technology to mitigate the risk of a PHI breach.
- Chapter Six: Insights from a survey on what is being done to secure PHI, what is not, and why.
- Chapter Seven: A description of PHIve, a 5-step method for assessing an organization's security risks, identifying gaps, and calculating the potential costs of a PHI breach.
- Chapter Eight: A demonstration of how PHIve works to estimate the financial costs of a PHI breach in terms of reputational, financial, legal, operational, and clinical repercussions. A detailed example of costing a PHI breach is given, including calculations and suggestions, and highlighting relevance and impact considerations.

The chapters are supplemented by a number of online appendices, hyperlinked to this report, which contain research notes from the various project subcommittees.

INTRODUCTION

The hope, and expectation, has been that driving health care entities to adopt electronic health records (EHRs) would reduce medical costs, provide for accessibility to health care information, and increase the quality of care. But the potential benefits of EHRs have been accompanied by an increase in the number of organizations handling protected health information (PHI) and, consequently, a rapidly growing volume of electronic health care data breaches.

Some of this can be attributed to insufficient training of staff and insufficient attention to preventive security measures. However, the substantial financial rewards for stolen health records also have grown, along with the ability of criminals to crack the security mechanisms designed to protect PHI.

Complicating matters is the fact that requirements for PHI protection have expanded beyond traditional provider and billing organizations involved in carrying out treatment, payment, or health care operations (covered entities) to include an increasing number of organizations supporting those covered entities in the handling of PHI (business associates). Many other organizations that are handling PHI today may not fit the regulatory definition of covered entities or their business associates, such as health exchanges, data miners, law firms, and other subcontractors. These participants in the health care ecosystem may not understand the requirements or the importance of protecting PHI.

Preventive measures such as security technology, policies, and procedures to protect PHI can be implemented to help mitigate risk and reduce either the probability or the impact of a PHI breach. Such measures may position an organization to improve care, strengthen its reputation, and benefit from operational efficiencies that can come from adopting EHRs. Without such safeguards, data breaches will continue to erode the public's confidence in the health care system and the expectation that the privacy of their health information will be protected.

So why have organizations not already fully implemented these preventive measures? A survey of participants in the health care industry, conducted in conjunction with the development of this report, provides insights into the challenges organizations face in strengthening their compliance programs. Despite a sense of having "effective policies" and taking "effective steps" toward compliance, respondents note a lack of both resources and leadership support as barriers to "ensuring requirements are currently being met."

But if healthcare industry leaders really understood the privacy expectations of their patients and customers and the repercussions and costs resulting from a PHI breach, as well as the advantages that increased security and HIPAA compliance could bring to their organizations, the return on investment (ROI) in strengthening their compliance programs would be far more attractive.

Nearly all health organizations will experience an electronic data breach in the next few years.

In fact, privacy and security programs would likely become a high priority if the health care industry more widely understood the increasing costs of class action lawsuits resulting from data breaches, not to mention the statistical probability that nearly all health organizations will experience an electronic data breach in the next few years.

To understand the value of PHI in an organization's care is to understand what is lost if that PHI is breached. This report provides a framework for calculating the cost of a data breach for any organization responsible for protecting PHI, thereby making a convincing case that achieving HIPAA compliance and data security is one of the best investments an organization can make.

The threats are real and ubiquitous, the risks are high, and the financial, reputational, and legal repercussions to individuals and organizations can be severe.

A Note about Terms before Getting Started

For purposes of this report, a shorthand definition of protected health information (PHI) is individually identifiable health information protected by any federal, state, or local law, rule, or regulation. Electronic protected health information (ePHI) would be PHI that is created, stored, or accessed through electronic means. Also, the terms "breach," "data breach," "privacy breach," "security breach," and "PHI breach" are used liberally and interchangeably within this report to describe the unauthorized disclosure of information that compromises the availability, integrity, or confidentiality of PHI.

It is recognized that there are other data beyond PHI that may simultaneously be breached that give rise to legal liability. Statutory and regulatory definitions are listed in Appendix A – Glossary of Terms and Acronyms.

CHAPTER ONE

The Progression of the Health Care Ecosystem

When the HIPAA Privacy statute was first enacted in 1996, most health information was on paper. In fact, even by 2006, according to a report from the Centers for Disease Control and Prevention (CDC) (see Figure 1 below), the use of electronic medical records (EMRs – the digital record of medical and treatment history of the patients in one practice) among office-based physicians in the U.S. stood at 29.2%. Only 12.4% of physicians used EMR systems with all four of the features considered necessary for a minimally functional system – systems allowing for computerized orders for prescriptions, computerized orders for tests, electronic viewing of test results, and electronic viewing of clinical notes.

Thanks to incentives for adoption and penalties for non-adoption under the Medicare and Medicaid programs, the use of EMRs grew significantly over time. By 2008, still only 41.5% of office-based physicians reported using any EMR system, but that is more than double the number in 2001.[1]

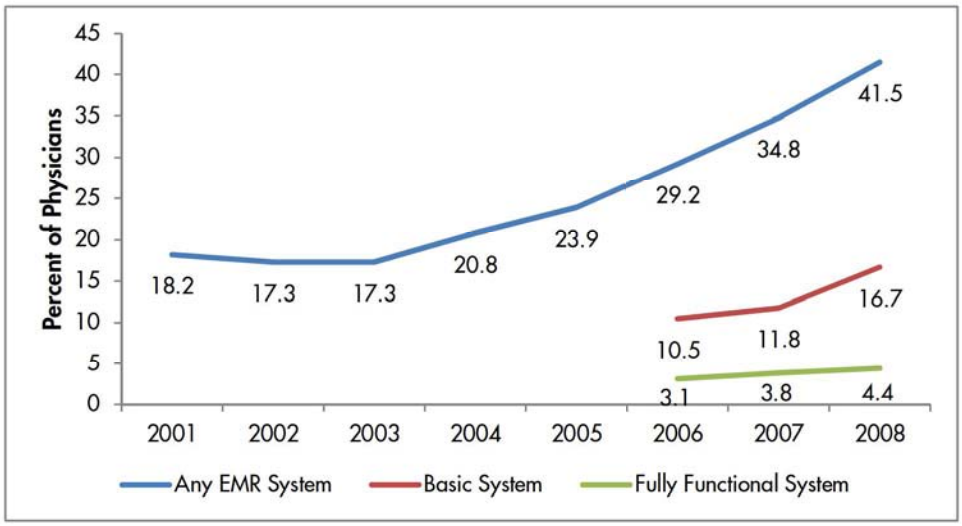


Figure 1: Percentage of office-based physicians with electronic medical record (EMR) systems: United States, 2001 - 2008

Notes: Any EMR is a medical record system that is either all or partially electronic (excluding systems solely for billing). Fully functional systems are a subset of basic systems. Excludes radiologists, anesthesiologists, and pathologists.
Source: CDC/NCHS, National Ambulatory Medical Care Survey

The Health Care Ecosystem 2012

The health care ecosystem is the arena in which health care services take place, comprised of individuals, providers, clinical support, payers, and others, including those that support the physical and electronic infrastructures, in addition to the information that is shared and that flows between them.

With the growth of electronic health records (EHRs – the evolution of EMRs to be more focused on the total health of the patient and designed to be shared with other health care providers), there has been a surge in the number of organizations that are now stakeholders in the health care ecosystem (see Table 1). These include new points of care (e.g., urgent care facilities, clinicians in retail stores, virtual offices associated with telemedicine delivered over the Internet), new business associates (e.g., revenue cycle companies, collections agencies), and organizations offering a myriad of electronic and web-based support services (e.g., data transmission, software-as-a-service and cloud computing, mobile devices, web portals).

These stakeholders are responsible for the confidentiality, integrity, and availability of all PHI they create, receive, maintain, transmit, or store. This responsibility includes implementing appropriate safeguards against any reasonably anticipated threats or hazards to the security or integrity of that information. They must ensure:

- **Confidentiality**: data or information is not made available or disclosed to unauthorized persons or processes;
- **Integrity**: data or information has not been altered or destroyed in an unauthorized manner; and
- **Availability**: data or information is accessible and useable upon demand by an authorized person.

Table 1: Stakeholders in the Health Care Ecosystem

Points of Care	Payers	Clinical Support	Business Associates	Others	IT Services
- Primary care physicians - Secondary physicians - OB/GYN physicians - Clinics - Hospitals - Therapists - Homeopaths - Long term care facilities - Rehab facilities - Assisted living - Urgent care facilities - Telehealth/ telemedicine - Retail physicians	- Primary insurers - Secondary insurers - Medicare - Medicaid - Employers: benefits administrators - Consumers	- Clinical labs - Research labs - Imaging companies - Pharmacies - Mail-order pharmacies - Phlebotomists	- Pharmacy benefits managers - Third-party administrators - Benefits administrators - Claims review/ utilization - Billing processors - Revenue cycle companies - Payment agencies - Collection agencies - Hospital discharge care support - Disease management companies - Wellness companies - Fulfillment companies - Health risk assessment organizations	- Life insurance companies - Law firms - Consultants - Auditors - Accreditation firms - Application trouble-shooters - Pharmaceutical/ medical device companies - Contract research organizations	- Data transmission (HIE) - Data storage - Data back-up - Data recovery services - Software as a service (SaaS) offerings - On-line diagnostic services - Mobile devices - Web portals: physicians - Web portals: consumers

The Ramifications

Electronic health information systems have become a "game changer" in the threat to health information privacy. In addition to the increase in the number of organizations that handle PHI and the increase in the financial incentives for medical identity theft, the frequency and the size of unauthorized PHI disclosures have continued to increase, along with the costs to the organizations unfortunate enough to have suffered such breaches.[2]

In the 15 years since the enactment of HIPAA, it has become evident that electronic health information technology offers the potential for future significant benefits, but it also has opened up the PHI universe to an increasing number of threats to the privacy and trust on which the health care delivery system is based. For the first time in the history of medicine, it is possible to:

- Improperly disclose identifiable electronic health information of millions of individuals "in a matter of seconds;"[3]
- Steal health information without having physical access to it and from locations that may be beyond the reach of U.S. laws;[4] and,
- Breach an individual's PHI in a manner that makes it impossible to restore.[5]

The threats to the security of PHI are not specific to one stakeholder group but are ubiquitous throughout the entire ecosystem due to the volume and availability of PHI data and transmission of electronic PHI records (ePHI). As depicted in Figure 2, the interrelationship of the stakeholders, the information flows of PHI, and the vulnerability/risk points indicate that the information is at risk whether in motion or at rest. At each instance, a copy of the data is created resulting in its residing in multiple databases and thereby providing greater vulnerability to threats.

Any organization or person that creates, handles, transmits, or stores PHI ("PHI protector"), regardless of size or function, is a member of this health care ecosystem and is responsible for the safeguarding of the PHI entrusted to its care, all under the watchful eye of legal and regulatory agencies.

The White House has recognized that the growing use of online transactions generally has increased "online fraud and identity theft," which "cost companies and individuals billions of dollars each year" and often "leave in their wake a mess of ruined credit and damaged finances that can take years to repair."

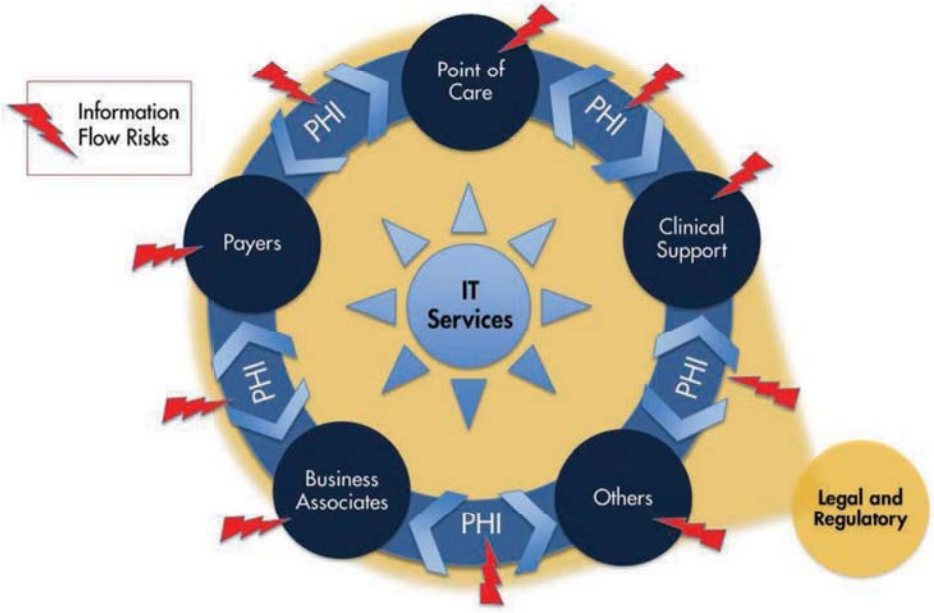


Figure 2: The health care ecosystem: stakeholders, information flows, and associated risks

In addition, "[t]he potential for fraud and weakness of privacy protections often leave individuals, businesses, and government reluctant to conduct major transactions online."[6] While the total potential cost and liability due to electronic fraud and privacy breaches has been difficult to quantify with precision, the White House has concluded that "the problem is real and it is increasing."[7]

The damage and liability that can result from electronic health information fraud and privacy violations are particularly acute. A stolen Social Security or credit card number can be replaced, but information about one's health status, once stolen, can be copied, altered, and circulated repeatedly. So the potential damage from a PHI breach to the individual and the payer is essentially unlimited.

Potential damage from a PHI breach to the individual and the payer is essentially unlimited.

As more individuals have become the victims of health information privacy breaches, public concern has grown, members of Congress have become involved,[8] state and federal laws protecting health information privacy have multiplied, enforcement of those laws has ramped up, and potential legal liability for violations of privacy laws has increased.

This growing risk of health information privacy liability is occurring at a time when there is significant pressure to reduce spending on health care.[9] In addition, the ability to protect health information has not matched the public's expectations for privacy, to the detriment of the finances and reputations of organizations in the health care ecosystem.

If PHI is not adequately safeguarded, the vision of a truly interoperable electronic health information system in the United States could be in jeopardy, just as it was a significant issue that contributed to Britain's decision to abandon its plans for a centralized electronic health information system.[10]

CHAPTER TWO

The Evolution of Laws, Rules, and Regulations

Management and reduction of the financial and business liability arising from mishandling PHI is only possible with a clear understanding of, first, the privacy rights of patients and customers, and, second, the requirements and enforcement mechanisms of health information privacy laws and professional ethics. In other words, enterprises that handle health information must be aware of consumer privacy rights and expectations in order to meet them.

The public's perception and expectation of a right to health information privacy is rooted in standards of professional ethics, has been read into (or some would say is "found within the 'penumbra' of") the U.S. Constitution, and is recognized in each state's tort law. Accordingly, a PHI protector must be cognizant of these expectations and how they influence the regulatory environment.

The Supreme Court has repeatedly recognized that individuals have a right to informational privacy that is protected from government violation by one or more sections of the Constitution and that, whatever its scope, the right appears to encompass health care information.[11] According to the Court, the right to privacy is "older than the Bill of Rights – older than our political parties, older than our school system."[12] The Constitutional privacy protection is strongest where the individual has a "reasonable expectation of privacy" in the health information arising from his or her personal health care.[13] Generally, "the more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny."[14] Information about mental health treatment, sexual orientation and conditions, physical defects or disabilities, or other clinical treatment detail is typically viewed by courts as more intimate and personal.

While the Constitution only protects an individual's right to informational privacy against federal and state governments, this right creates an expectation that the individual has a more general right to privacy, which is, in fact, protected by other laws. States, too, have recognized an individual's right to privacy, holding individuals and organizations accountable for breaches of privacy under various tort law theories and pursuant to state statutes. Many of the headline-grabbing financial settlements related to privacy breaches stem from lawsuits based on state tort law.

A constitutionally based right to privacy for sensitive personal information has also been recognized by the other two branches of the federal government – Congress, and the Executive Branch through the U.S. Department of Health and Human Services (HHS).

According to Congressional findings, Americans expect a right to privacy for personal information about themselves that is a "personal and fundamental right protected by the Constitution of the United States."[15] HHS has determined that "privacy

is necessary to secure effective, high quality health care."[16] Further, in the HIPAA Privacy rulemaking, the right to privacy of highly personal information is a "fundamental right" of all Americans[17] and "one of the key values on which our society is built."[18]

Although protection requirements for PHI evolved slowly at first, in recent years they have expanded dramatically as EHRs have been more widely adopted. When HIPAA was enacted in 1996, only covered entities were subject to established standards for the privacy and security of PHI. Since then:

- Detailed HIPAA Privacy and Security regulations were issued, subjecting only certain "covered entities" to both privacy and security standards;
- The *Genetic Information Non-Discrimination Act of 2008* has been enacted, affording special privacy protections for genetic information; and
- The *American Recovery and Reinvestment Act of 2009* was passed, which included:
  - incentives for health care providers and practitioners to adopt EHRs, and
  - the *Health Information Technology for Economic and Clinical Health* (HITECH) *Act* that enhanced the health information privacy rights of individuals, and the penalties for those who violate those rights, and extended HIPAA privacy and security standards (and penalties) for ePHI to "business associates" of covered entities.

Table 2: A summary of the HIPAA laws, rules, and regulations

1996 HIPAA Subtitle F:

HHS secretary is required to establish standards for the privacy and security of PHI held by covered entities (CEs).

2000 (amended 2002) HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164)

Defined requirements for the protection of individually identifiable health information held by covered entities (protected health information or "PHI") and gives individuals specific rights with respect to that information

Requirements of covered entities:

- May not use or disclose PHI except as permitted or required by the Privacy Rule
- 2005: Established obligations of business associates (BA)
  - Required CE to obtain contractual and satisfactory assurances that the BA will safeguard PHI
  - Established permitted and required uses and disclosures, return, and/or destruction for BA
  - Authorized termination of contract by CE if BA violated material term of contract

Rights of individuals:

- Be informed of CE privacy practices and privacy rights
- Obtain a copy of their medical records
- Amend incomplete or incorrect health information
- Learn of certain disclosures of their PHI made by a CE or BA
- Applies to all forms of PHI (electronic, written, or oral)

2003 – 2010 HHS Office for Civil Rights (OCR) Privacy Rule Compliance Investigations

Most common types of CEs required to take corrective action (in order of frequency):

- Private practices
- General hospitals
- Outpatient facilities
- Health plans
- Pharmacies

Issues investigated most by OCR (in order of frequency):

- Impermissible uses and disclosures of PHI
- Lack of safeguards of PHI
- Denial of individuals' access to their PHI
- Uses or disclosures of more than the minimum necessary PHI
- The inability of individuals to file complaints with CEs

2003 HIPAA Security Rule (45 CFR 160 and Subparts A and C of Part 164)

Established national standards to protect electronic PHI created, received, used, or maintained by a covered entity

Requirements of covered entities:

- Requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI
- Required to be in compliance with the Security Rule by April 20, 2005

Enforcement authority:

- 2003 to July 27, 2009: HHS delegated authority to administer and enforce the Security Rule to the Centers for Medicare & Medicaid Services.
- July 27, 2009 – present: HHS transferred authority to OCR

2005 – 2010 OCR Security Rule Compliance Investigations

Issues investigated most by OCR (in order of frequency):

- Failure to demonstrate adequate policies and procedures or safeguards to address response and reporting of security incidents
- Security awareness and training
- Access controls
- Information access management
- Work station security

2009 HITECH Amends HIPAA (Title XIII of Division A and Title IV of Division B of ARRA)

Provides incentives to providers to allow for implementation and utilization of electronic health records

Meaningful use:

- Provision is made for incentive payments to eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) who participate in the Medicare and Medicaid programs and who adopt and successfully demonstrate the meaningful use of certified electronic health records (EHRs)

Details of incentives:

- Federal incentive payments available to doctors and hospitals upon:
  - Adoption of EHRs and
  - Demonstration of improvements in quality, safety, and effectiveness of care
- Medicare: if eligible, up to $44,000 over 5 years
- Medicaid: if eligible, up to $63,750 over 6 years
  - 1st year: for adopting, implementing, and upgrading certified EHR technology
  - Subsequent years: for demonstrating meaningful use

2009 HITECH Amends HIPAA (Title XIII of Division A and Title IV of Division B of ARRA), *continued*

Modifies and enhances HIPAA privacy, security, and enforcement standards for PHI that were applicable to covered entities and makes certain standards and penalties applicable to business associates

Interim Final Rule requirements:

- 2009: Compliance with Breach Notification Rule required of both CEs and BAs

2010: Proposed modifications to HIPAA:

- Penalties
- Compliance reviews and audits

2011: Accounting for disclosures:

- Expanded individual rights to obtain report of access to PHI (effective 2013 for records acquired before 2009; and 2014 for records acquired during or after 2009)
- Reduced number of years of accounting from 6 to 3
- Reduced number of days required to respond by CE from 60 to 30
- Extended requirements to BAs

It can be expected that additional regulations will come and more entities will be held responsible, as the existing laws are, in many cases, non-specific or conflicting, and leave gaps in responsibility. For example:

- The HIPAA Privacy and Security Rules only apply to "covered entities" and their "business associates," but health information is handled by many other individuals and entities,[19] including subcontractors to business associates.
- The Data Breach Notification Rule does not specify breach notification requirements for data breaches caused by researchers, law officials, or those who subpoena records.
- The Privacy Rule requires covered entities to inform individuals "in plain language" of their health information privacy rights but does not list the right to health information privacy among those rights.[20]
- The HIPAA Privacy and Security Rules and the "Privacy" section of the HITECH Act contain definitions of key terms but do not define "health information privacy."[21]
- The HIPAA Privacy Rule provides that covered entities and their business associates may use and disclose an individual's identifiable health information without consent (even over the individual's objection) for treatment, payment, and health care operations, but standards of professional ethics, which HHS says "retain their vitality," have traditionally prohibited such disclosures with narrow exceptions.[22]

A former head of HHS's Office of Health Information Technology stated that "HIPAA makes no sense" in the current environment because it did not anticipate that health information would pass through many hands.[23]

More information is available in Appendix B – Legal and Regulatory Liabilities.

CHAPTER THREE

PHI Data Breach Landscape

The number of Americans that have become victims of health information privacy breaches has grown rapidly with the adoption of EHRs.

- Between 2005 and 2008, nearly 230 million electronic records were breached including almost 39.5 million electronic health records.[24]
- In the past two years, the health information privacy of nearly 18 million Americans has been breached electronically, which is "equivalent to the population of Florida."[25]
- In the period September through November of 2011:
  - A government benefits program suffered the theft of electronic health records of 4.9 million military personnel;[26]
  - A reputable West Coast health care system experienced the electronic theft of health information for 4 million of its patients;[27] and
  - A major academic medical center inadvertently disclosed the electronic health records of 20,000 of its patients.[28]
- In a November 2011 survey completed by 72 provider organizations conducted by Ponemon Institute, 96% reported having had at least one data breach in the past 24 months. On average, health organizations have had four data breach incidents during the past two years. Compared to the prior year, there were increases in both the frequency of data breaches (up 32%) and the average economic impact of a breach (up 10%). The average number of lost or stolen records per breach also increased (2,575 compared to 1,769 the year before). In addition, there was a 26% increase in respondents who said their data breaches led to cases of identity theft. Notable was the percentage of organizations fully implementing or in the process of implementing an electronic health records system, which increased from 56% last year to 66% in this year's study.[29]

Health information privacy violations that in the past typically involved lost or misplaced information increasingly involve medical identity theft by organized crime that is difficult to detect and correct.[30] According to 2010 reported data collected by the Identity Theft Resource Center, data breaches are occurring in health care at nearly three times the rate as in banking and finance.[31] This may be due to more intense reporting requirements in health care, the greater number of people who have access to health data, and the growing black market for patient medical information.[32]

While the reason for stealing medical records may be baffling to some, it certainly is not to those who are profiting from those illegal activities.

Fraud resulting from medical identity theft primarily takes two forms: (1) physician identification numbers that are stolen and used to bill for services, and (2) patient identification information that is stolen (or lent to friends and relatives) and used to obtain services or to bill for services.[33]

In a survey of 600 executives from hospitals, physician groups, health insurance companies, and pharmaceutical and life sciences companies, PricewaterhouseCoopers (PwC) found that 36% of the surveyed hospitals and physician groups said patients had sought services using somebody else's name and identification.[34]

At approximately $60 billion per year, Medicare fraud has become "one of, if not the most profitable, crimes in America." In south Florida, Medicare fraud has replaced cocaine as the major criminal enterprise.[35]

Further evidence of the scope and implications of clinical fraud is gleaned from early fraud analysis, which has led to estimates of emergency department, emergency services clinic, and hospital inpatient clinical fraud rates of between 2-10% of all patients treated. That analysis revealed that the majority of clinical fraud is perpetrated in an effort to obtain prescription narcotics for illegitimate use, but up to 5% of clinical fraud appears to be perpetrated for receipt of free health care. In both scenarios, the impact on the PHI breach victim whose information is used to commit clinical fraud comes in the form of monetary loss, possible inability to obtain or retain insurance, and corruption of medical history. Damage done to the victim can eventually impact the facility where the breach occurred as the victim seeks reimbursement or sues for damages.[36]

On average, medical ID theft results in a payout in excess of $20,000.

Put It This Way

- A thief downloading and stealing data can get $50 on the street for a medical identification number compared to just $1 for a Social Security number. For those receiving the medical ID number and using it to defraud a health care organization, the average payout is more than $20,000, according to Pam Dixon, executive director of the World Privacy Forum. Compare that to just $2,000 for the average payout for regular ID theft.[37]
- A clerk in a medical clinic in a Florida hospital stole the medical IDs of 1,100 patients and sold them. The numbers were subsequently used to bill Medicare for $2.8 million in false claims.[38]
- A hospital in Orlando, Florida, fired three employees for improperly reviewing emergency department records of 2,252 patients, reportedly to forward information about accident victims to lawyers.[39]

What about Snooping?

In a 2011 survey conducted by Cyber-Ark of 1,422 IT staff and C-level professionals across North America, Europe, the Middle East, and Africa (EMEA), 28% of North American IT staff respondents admitted to snooping while 44% of EMEA IT staff admitted the same.[40] In a patient privacy breach study of compliance and privacy officers at mid-to-large-size hospitals and health care service providers, Veriphyr, a vendor of data analytics software that generates access activity logs of patients' medical records, found that 35% of studied breaches "involved snooping into medical records of co-workers and 27% involved viewing records of friends and relatives."[41] And when it comes to the medical records of celebrities?

- The *Los Angeles Times* reported that hospital officials from UCLA Medical Center fired a member of its staff who reviewed a prominent celebrity's records without authorization.[42] The employee was paid $4,600 by the *National Enquirer*.[43]

- The *Arizona Star* reported that the University Medical Center in Tucson, where Representative Gabrielle Giffords was taken following the shooting rampage that left her injured, fired three employees for allegedly accessing confidential medical records inappropriately.[44]

How Do People Feel about Breaches?

Not surprisingly, the frequent reports of massive breaches of electronic health information have eroded the public's confidence in the ability of health care providers and organizations to protect the privacy of PHI. Approximately 69% of Americans have heard of, or read of, health records being stolen from health care providers.[45] A majority of Americans (54%) only trust their health care providers "somewhat" to protect the privacy of their health care information, and nearly 60% believe that their medical records are not adequately protected by existing laws.[46]

Nearly 60% of Americans believe that their medical records are not adequately protected.

The National Committee on Vital and Health Statistics – designated by HIPAA to provide advice on implementation – found after months of hearings that "public trust is lacking," and that the benefits of electronic health information are unlikely to convince individuals to take the personal risk of making their health information available over a National Health Information Network.[47] HHS findings confirm that Americans believe they have a right to privacy for their health information and that it should be protected as the nation moves toward adopting electronic health information technology.[48] An online poll of 2,000 adults revealed that 97% of the public believe health care providers and insurers should not be able to share their health information without their consent.[49] According to HHS, the lack of public confidence in health information privacy protection will drive up the cost of health care.

In the beginning, HHS estimated that the HIPAA Privacy Rule would add $18 billion to health care costs over the period 2003 through 2013.[50] However, HHS assumed that much of this cost would be offset by the savings that would be achieved if people were more willing to obtain preventive health care and treatment due to their belief that "their information will be used properly and not disseminated beyond certain bounds without their knowledge and consent."[51] For example, HHS has found that nearly $800,000 could be saved annually by convincing the more than two million Americans who fail to seek treatment for mental illness due to privacy concerns to seek needed treatment.[52] Hundreds of millions of dollars more could be saved annually by adopting privacy measures that would encourage those with HIV/AIDS and other sexually transmitted diseases to seek diagnosis and treatment.[53] Those anticipated savings will not be achieved unless the public believes the privacy of their health information will be protected in electronic health information systems.

On the Horizon

The White House has outlined a national strategy for addressing the growing fraud and privacy problems with electronic information systems that has as its guiding principle "[t]he enhancement of privacy and support of civil liberties."[54] That strategy calls for adopting electronic identity solutions that are privacy-enhancing, secure, resilient, interoperable, cost-effective, and easy to use.[55] The strategy will take "many years" to develop and will require the "dedicated efforts of both the public and private sectors."[56] So it is unclear whether the schedule for implementing such a strategy is consistent with the goal in the HITECH sections of the *American Recovery and Reinvestment Act of 2009* to achieve widespread adoption and meaningful use of electronic health records by 2014.[57]

In summary, the right to health care privacy exists and the organizations that handle PHI are legally and ethically responsible for protecting it. There are bad-intentioned people who are focused on stealing that data, as well as good but untrained people who are not aware of their responsibilities and the means of protection.

The balance of this report will help PHI protectors to:

1. Provide suggested safeguards and controls to protect against threats and related vulnerabilities.
2. Recommend a scale for determining "unacceptable" levels of risks.
3. Identify the sources and range of financial costs, reputational harm, and legal liabilities that can arise from violations of the expectation and trust that PHI will be protected.
4. Provide a tool for quantifying the financial impact to the organization should a breach occur.
5. Build a robust business case for investing in enhanced PHI security.

CHAPTER FOUR

Threats and Vulnerabilities

Eleven Elements That Threaten the Security of PHI

While security threats and vulnerabilities to the confidentiality and integrity of PHI are well documented and are generally independent of what part an organization plays within the health care ecosystem, an analysis of the most recent data breaches highlights the following major contributors:

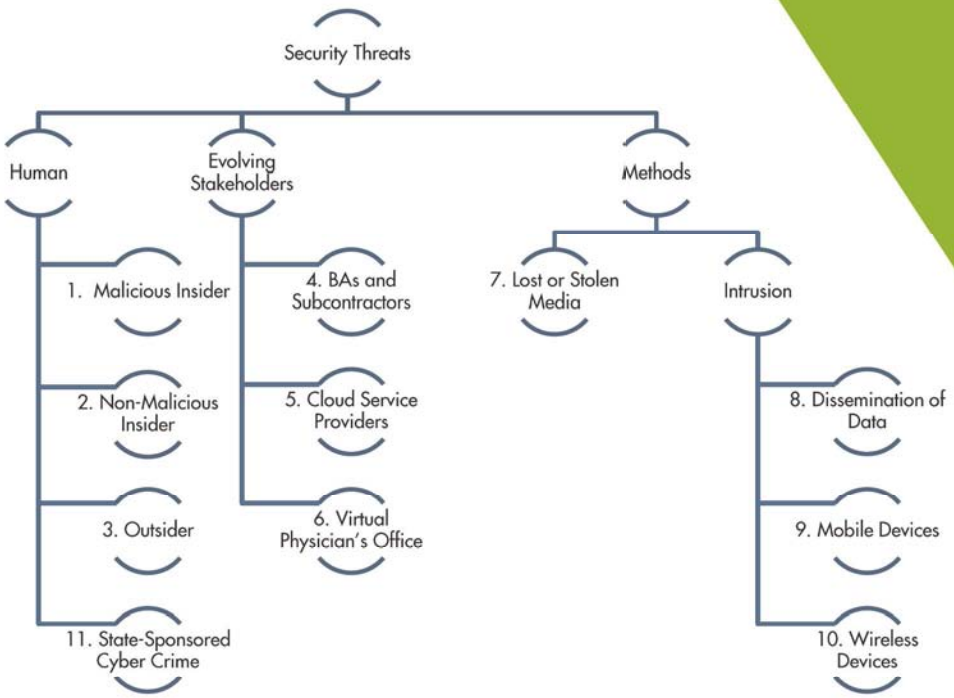


Figure 3: Top 11 elements threatening PHI security

- The "Insider" is a current or former workforce member (employee, contractor, or temporary staff) who is known as a **Malicious Insider (1)** or a **Non-Malicious Insider (2)**, depending upon intent. The non-malicious insider is typically an authorized user who causes the accidental disclosure of PHI due to human error or lack of training. The malicious insider is intent on breaching security controls to gain access to or manipulate PHI in order to harm or disrupt the organization or for personal gain. According to Verizon's 2010 Data Breach Investigations Report, almost half (48%) of all data breaches involve the participation of an insider, but only 10% are unintentional – whereas 90% are deliberate and malicious and usually involve misuse of privileges. Of the crimes tied to insiders, almost one-quarter (24%)

Almost half (48%) of all data breaches involve the participation of an insider, but only 10% are unintentional – whereas 90% are deliberate.

were perpetrated by employees involved in a job change, such as those newly hired, the recently promoted, or those being fired or resigning.[58] Insiders can be the most dangerous of attackers as they are usually familiar with organizational policies, procedures, authorization codes, file systems, and system access, and they are most likely to know how to cause the most damage.

- The **Outsider (3)** is a non-workforce-member who is intent on disrupting the organization or gaining access to PHI for nefarious purposes. The outsider threat can use many techniques to gain access to PHI, including computer viruses, Trojan horses, worms, social engineering, IP spoofing, mail bombing, password cracking, or packet replay or modification, among other methods. The "hacktivist" group Anonymous recently focused their efforts on a computer crimes investigator, hacking into his emails, voicemails, and SMS text messages, posting 38,000 emails containing "computer forensics techniques, investigation protocols as well as highly embarrassing personal information."[59]

- Some of most significant breaches in terms of number of records lost are caused by **Lost/Stolen Media (4)**. The typical example is a lost backup tape or a stolen laptop. Findings in a PwC survey indicated that "theft accounted for 66% of reported health data breaches in the past two years."[60] Recently, a thief stole medical information of more than four million patients of Sacramento-based Sutter Health by the simple act of breaking a window with a rock and stealing a desktop computer at the affiliated Sutter Medical Foundation.[61]

- Many breaches occurring in the health care ecosystem are caused during the **Dissemination of Data (5)** between stakeholders of the ecosystem. This involves the use of technologies with weak controls, such as FTP (file transfer protocol) sites, which lack the security, tracking, and auditing capabilities of sFTP (secure file transfer protocol) to ensure the protection of health information. "Drug development data, clinical trial data, health records, billing information, X-rays, MRIs, and social security numbers are some of the types of highly sensitive data that are at risk of exposure simply because they are being exchanged frequently among multiple third parties."[62] Organizations involved in the transmission of data must invest in technology and processes that protect the data in transit and at rest, while providing the ability to manage and audit data transfers between business partners, service providers, and customers.

- As the size and price of portable electronic communication devices continue to decrease, we now find that many health care staff have access to PHI using **Mobile Devices (6)** (e.g., PDAs, iPads, flash memory cards, etc.). These devices do not have the mature security controls commonly found in computer systems. Between September 22, 2009, and May 8, 2011, mobile devices were responsible for 116 breaches, exposing the PHI of more than 1.9 million patients.[63] According to a recent Manhattan Research study, "64% of physicians own smartphones and 30% of physicians have an iPad, with another 28% planning to buy one within six months. Ten thousand mobile health care applications are available today on the iPad, with a larger [sic] number of them created to provide access to electronic health records. Additionally, one-third of physicians use their mobile devices to input to EHRs while seeing patients, while the information is fresh."[64] In the November 2011 Ponemon study, 81% of participants reported the use of mobile devices to collect, store, and/or transmit some form of PHI, yet 49% admitted their organizations do nothing to protect these devices.[65] Similarly, 55% of those participating in the previously cited PwC survey said that privacy and security issues associated with mobile technology had not yet been addressed.[66]

- Outsourcing has grown exponentially over the past fifteen years and is common within the health care ecosystem. **Business Associates, Suppliers, Vendors, and Partners (7)** are subject to exactly the same threats as the health care provider. The contract or other arrangement between a covered entity and business associate must provide that the business associate will use appropriate safeguards to prevent use or disclosure of PHI and establish permitted and required uses and disclosures, among other requirements.[67] Not only were business associates involved in more than 20% of all PHI data breaches,[68] the top-three breaches in terms of the number of individuals affected involved BAs and represented more than 45% of all individuals that have been reported to HHS as being affected – TRICARE, 4.9 million

affected, September 2011; Health Net, 1.9 million affected, January 2011; and New York City Hospitals Corp., 1.7 million affected, December 2010. And yet, only 36% of health organizations perform a pre-contract assessment of their business associates, and only about 25% conduct post-contract compliance assessments.[69]

- As providers of storage and transmission services for PHI, **Cloud Providers (8)** must protect against the multiple opportunities for physical and electronic breaches. The ascent and prominence of this newest generation of outsourcing services used by organizations in the health care ecosystem has resulted in a potential increase in risk to the security of PHI data. That risk comes from a number of security vulnerabilities:
  - Hacking from publicly available interfaces to the network;
  - Electronic access to sensitive information stored on common servers by different organizations;
  - Physical access by multiple parties, as cloud providers may have a number of storage locations; and
  - Inconsistent rules for data protection and data breaches across geographic regions.[70]

The popularity of cloud computing is based on the cost efficiencies of outsourcing both the storage and the security compliance requirements. The widely held belief that security at a cloud computing service, uncontrolled by the covered entity, potentially can be compromised has done nothing to slow the swift adoption of cloud computing usage. The National Institute of Standards and Technology (NIST) has finalized its first set of guidelines for managing security and privacy issues in cloud computing (NIST Special Publication 800-144).[71] This publication provides an overview of the challenges of public cloud computing to privacy and security, and highlights considerations when outsourcing to a public cloud environment. According to Gartner Group, cloud computing is expected to represent a $150 billion market by 2014.[72] The net result of employing cloud computing services for the maintenance of PHI data has been to add another layer of potential breach exposure to a health care organization. Ultimately, the consumer of the cloud services retains full legal responsibility for compliance with any applicable statutes and regulations.

Ultimately, the consumer of the cloud services retains full legal responsibility for compliance with any applicable statutes and regulations.

For more information, read Appendix C – Legal Considerations with Respect to Cloud Computing.

- Understanding the vulnerabilities created by new technologies, as well as evolving motives, is critical for establishing appropriate safeguards to prevent disclosures of PHI. These vulnerabilities include the difficulty in providing safeguards for the Virtual Physician's Office and Wireless Health Care Device Technology, and against State-Sponsored Cyber Crime.
  - **Virtual Physician's Office (9)** and **Wireless Health Care Device Technology (10)**: No longer limited to a face-to-face consultation, the doctor-patient relationship has moved out of the doctor's office or clinic and into cyberspace, bringing along with it issues related to the legal protections of physician-patient privilege and privacy, and online data protection. Email, texting, video conferencing, digital medical cameras, digital stethoscopes, diagnostic equipment, and remote monitoring are altering the traditional method of delivering medical care with real-time diagnostics and increased transmission of patient data.

    Millions of Americans now rely upon the Internet as a primary source of medical information or education about their own symptoms, conditions, diagnoses, and treatments. The practice of telemedicine – consulting with another physician by using technology – is constantly evolving and expanding into areas never before imagined. Physicians are establishing their own web sites and some are now practicing medicine on the Internet. The practice of medicine has now evolved to include interactions that might not ordinarily have been considered to have the legal protections of doctor-patient privilege. These interactions are, at times, both real and virtual, and the consumer-patient is now in a situation where it is difficult to identify exactly who is the party on the other end or where their information is being sent.[73]

- **State-Sponsored Cyber Crime (11)**: State-sponsored cyber attacks are on the rise and the Pentagon has concluded that "computer sabotage coming from another country can constitute an act of war," allowing the U.S. to respond using military force.[74] Here are some examples:
  - Operation "Shady Rat" breached networks of 72 organizations across the globe;
  - Foreign hackers stole 24,000 sensitive files from the Pentagon in a single breach;
  - "Aurora" attacks targeted Cisco, Juniper, Google, and Adobe;
  - "Night Dragon" attacks targeted global oil and gas data.[75]

  Although careful not to mention any specific countries, British Foreign Secretary William Hague closed a two-day conference on cybersecurity with a warning to foreign governments that a more confrontational approach will be undertaken if state-sponsored cyber-attacks do not stop.[76]

The following scenario is representative of a compilation of recent security breaches, along with repercussions that can follow, and preventive measures that could have been taken. According to HIPAA regulations, covered entities must ensure protections for PHI in a business associate agreement when outsourcing services to business associates, suppliers, vendors, and partners who create, receive, maintain, transmit, or store PHI. The legal responsibility for a data breach caused by a business associate belongs to the covered entity, and that, along with the resulting financial ramifications, should not be underestimated.

PHI Threat Scenario: Business Associate

In this scenario, a major New York City hospital server housing a database of over 845,000 patient records could no longer be accessed due to the mechanical failure of the hard drives. The IT manager followed procedures to restore the database from the hospital's magnetic backup tapes, but the backup tapes were blank.

The permanent loss of the database records would put the hospital in clear violation of HIPAA data retention and availability requirements. To restore the server, the IT manager contracted with a local third-party data recovery service provider. With no documented policy or procedure for assessing the capabilities and security compliance of such service providers, the IT support manager selected the company based on their 48-hour turnaround time, and shipped them the damaged hard drives without vetting their data security protocols.

The data recovery was a complete success. Within two days, the recovered data was returned to the IT support manager who uploaded the full database of patient records onto the hospital's new server and the tape backup system was fully functional again. The IT manager made a note in his files to use the local data recovery service provider again, thinking all had gone quite well.

But all was not well. Several months after the recovery, the hospital discovered that a breach of PHI had occurred during the recovery process. While creating an image of all the data on the drives, the data recovery engineer discovered the database of PHI records, including financial and health care account information. He made a second copy of the database for himself, found the records of a female patient with a description closely matching that of his ailing wife, and altered them to fit his wife's description perfectly, removing references to the female's blood type and life-threatening allergy to insulin. His wife used the fraudulent identity to receive surgical treatments for cancerous tumors in her lungs. The engineer used the credit card data found in other records to pay for the surgery, pharmaceuticals, and rehabilitation.

Several of the hospital's patients began reporting unauthorized purchases on their credit cards. The cause of the security breach was not discovered until the woman whose record was altered received emergency surgery after a car crash. Unconscious when she arrived at the hospital, she died from anaphylactic shock during a simple surgical procedure – an allergic reaction to the insulin she was administered during the operation.

The husband was convinced that his wife's allergy to insulin was well documented in her health record. After investigating the woman's health records more closely, it was discovered that her PHI recently had been altered and the changes were traced back to the NYC hospital's database. The hospital's forensic team was called in, and the breach was traced to the third-party data recovery service provider and their unscrupulous data recovery engineer, who, it was then revealed, had not been subjected to a background check upon hiring. The data recovery engineer had a criminal history of identity theft.

Reports of the breach, the altered medical records, and the woman's death were picked up by the media. The hospital posted a public notice of the PHI breach and notification letters were sent to all impacted patients outlining the details of the breach, the PHI disclosed, and who had handled their data. Two years of credit monitoring and fraud resolution services, along with credit and identity theft restoration if needed, were offered by the hospital to all affected individuals. However, the larger threat to the patients was the misuse of their PHI which had gone unmonitored. The hospital's brand name and image were damaged severely.

An internal study was conducted at the hospital and new protocols were adopted to mitigate the risk of using third-party data recovery vendors. The hospital's risk management process was updated and the hospital's chief information security officer (CISO) and the IT manager were fired.

Repercussions of This Scenario

Reputational Repercussions

- Tainted the hospital's brand and reputation, resulting in a loss of current patients and associated revenue due to the availability and acceptability of other hospitals in the New York City metropolitan area
- Loss of expected level of new patients due to reputational loss
- Loss of one surgeon, who went to work for another hospital due to reputational loss

Financial Repercussions

- Cost of corrective action plan including:
  - Cost of developing, documenting, implementing, and training on new processes and procedures related to contracting with third-party service providers
  - Cost of reconstructing altered records to ensure accuracy for affected individuals
  - Cost of incremental staff for auditing policies and procedures
  - Cost of new hard drives
- Cost of providing ID theft monitoring, fraud resolution services, and credit and ID theft restoration services to affected individuals for two years
- Cost of communications to affected individuals, HHS, and state agencies, including legal review, data management, and postage
- Cost of public relations campaign including content development, legal review, and advertising
- Cost of replacing data back-up services vendor

The financial implications of reportable PHI breaches extend beyond the federal and state fines and penalties to include a myriad of cash and non-cash costs.

Legal/Compliance Repercussions

- HHS Office for Civil Rights (OCR) fines
- State fines
- Loss of payment card industry attestation and cost of re-establishing accreditation
- Lawsuit related to stolen credit cards
- Insurance deductible
- Cost of re-instatement of PCI accreditation

Operational Repercussions

- Cost of new CISO and new IT manager, including recruiting, relocation, and higher salary
- Cost of additional IT security workforce member to audit policies and procedures and deliver training

Clinical Repercussions

- Cost of 14 cases of fraudulent claims processed

The total cost to the organization as a result of this hypothetical breach was over $25 million. (See the details of the costing of this scenario in Chapter 8: Calculating the Cost of a PHI Breach Using PHIve.)

Preventive Measures Related to This Scenario

Policy

- Vetting guidelines that include: third-party verification of the service provider's data security protocols; proof of compliance with HIPAA/HITECH data privacy/protection guidelines; certification of a secure network; background checks on all employees who handle drives and data during the recovery process; training of recovery engineers to safely manage encryption keys; non-disclosure agreements; and chain-of-custody protocols
- All business associates evaluated by the covered entity's vendor risk assessment program and include a full security program review
- Mandatory update of security reviews of business associates at least annually

Procedures

- Defined, documented, and repeatable business associate risk management processes
- At least an annual review of business associate security practices
- Strong enforcement practices for failing to adhere to the organization's policies

For more information, read Appendix D – PHI Threat Scenarios.

CHAPTER FIVE

Safeguards and Controls

At the 2011 annual meeting of the Office of the National Coordinator for Health IT, Leon Rodriquez, the recently appointed director of HHS's OCR, provided this advice to health care organizations to improve HIPAA compliance and the security of PHI:

- Check that risk assessments are up to date;
- Make sure senior managers are supportive of risk mitigation strategies;
- Review existing compliance programs as well as staff training;
- Ensure vigilant implementation of privacy and security policies and procedures, as well as tough sanctions for violating them;
- Conduct frequent internal compliance audits; and
- Develop a plan for prompt response to breach incidents.[77]

Director Rodriquez's statements underscore the need for an enterprise-wide risk management approach. Too often, information security is viewed solely as an IT (information technology) problem. However, such a view is too narrow and masks the larger organizational responsibility.

Information security vulnerabilities hold for the entire enterprise, and lack of recognition of this can result in enterprise under investment in PHI security. Businesses can substantially reduce the negative consequences of a successful cyber incident through risk management across the entire organization.

In 2008, the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) published *The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*, (document available on request) and in 2010, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (document available at webstore.ansi.org/cybersecurity).

Together, these publications provide a detailed framework that reviews cybersecurity on an enterprise-wide basis, analyzing cyber issues from a strategic, cross-departmental, and economic perspective. Such a framework allows for better analysis of all aspects of the issue so that it can be better understood, managed, and invested in by CFOs and other senior executives.

While a compliance program developed by such a cross-departmental team will be unique to each organization based on the differing business and security needs, there are three aspects of any compliance program that will help to mitigate the risk of a data breach:

Policy

Privacy policies contain the overarching principles embraced by the executive members of an organization that establish both the culture as it relates to the importance of safeguarding PHI and their expectations of employees, subcontractors, providers, and business associates. Visible executive support can be formalized through the establishment of a privacy office and active participation by the executive team on a privacy steering committee. Committee membership typically can include the general counsel, compliance officer, privacy officer, security officer, chief medical officer, chief information officer, chief financial officer, and human resources.

Security breaches can frequently stem from unintentional errors and lack of awareness.

A common framework for information security management – such as the ISO/IEC 27001 and 27002 standards[78] and NIST Special publication 800-30[79] – provides a model for business controls that embody these policies and which can be applied to:

- protection of PHI;
- detection of, and incident response to, a breach; and
- recovery of PHI.

Also notable are ISO 27799[80] and the HITRUST Common Security Framework,[81] which apply this framework specifically to the health care sector.

Procedures

Procedures must be developed, documented, and implemented to ensure the effectiveness of the key controls in the policies. Training in an organization's policies and procedures is imperative to minimize the possibility of one of the most common security breaches: unintentional errors and lack of awareness, typically at the hands of a "non-malicious" insider. Without a strong enforcement program and sanctions for non-compliance, the documentation and implementation of procedures will be ineffective.

It is critical that the executive team actively and visibly supports the policies, and that adherence to the procedures is expected. Investments made in the development, communication, and training of the security program in combination with effective enforcement and sanctions will strengthen the compliance program and provide for the greatest protection of PHI.

Procedures must be augmented by security technologies and address their effectiveness. Investments in security technologies that are either not implemented or ignored by the staff are worthless. Examples include:

- Virus protection turned off by an employee which leaves the system vulnerable to attacks;
- Installed encryption technology without a procedure to encrypt the data; and
- Access controls that are not updated upon job change or termination.

Technology

Examples of the more common information security technical safeguards required in the HIPAA Final Security Rule 164.312 include:

- **Access Control**: Protect ePHI from unauthorized disclosure
  - Allow system access only to authorized persons or applications
  - For a web environment, implement a web access management solution
  - Consider role-based access control
  - Assign unique user identification
  - Ensure the use, monitoring, and audit recording of emergency credentials
  - Establish automatic logoff and re-authentication after a period of inactivity
  - Limit access to encrypted applications to those who can decrypt the data
- **Integrity of Audit Controls**: Protect information from alteration or destruction
  - Implement mechanism to authenticate ePHI
  - Implement methods to corroborate that information has not been altered or destroyed
- **Transmission Security**: Protect ePHI that is being transmitted over a network
  - Consider encryption for best protection and safe harbor
  - Ensure strong encryption up to 2048 bits (asymmetric) and 128 bits (symmetric)
  - Verify data integrity with digital signatures or SSL certificates

In Figure 4 the relationship between policy, procedure, and technology is illustrated for each of the eleven major elements that threaten the security of PHI. Note that policy plays an important role in all threats. Most elements have more than one component and the venn diagram illustrates the interaction between the components.

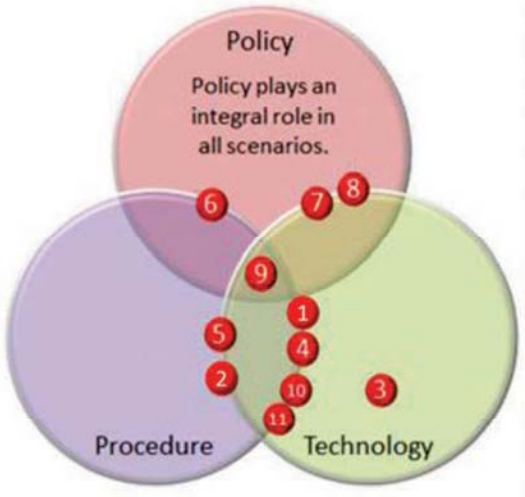


Figure 4: Preventive measures as related to the top threats

#1 Malicious Insiders: A strong awareness policy and training program is needed to train staff on how to recognize suspicious behavior, combined with Data Leakage Prevention (DLP) technology to prevent intentional disclosure.

#2 Non-Malicious Insider: A strong security awareness policy and training program is needed to educate staff on how to properly handle sensitive information, combined with DLP technology to prevent accidental disclosure.

#3 Outsider Threat: A number of technology preventive measures should be deployed including intrusion detection, virus protection, etc.

#4 Lost / Stolen Media: Preventive measures include technology such as encryption, key management, etc., combined with procedural controls, e.g., mandating staff to encrypt the PHI data and use strong passwords.

#5 Dissemination of Data: Technology controls include implementation of secure file transfer protocol and secure email. Procedures must be established to always use the secure file transfer and email when transferring sensitive information.

#6 Mobile Devices: A policy must be established on the proper use of mobile devices and staff must be trained on the new policy. Implement new technology that provides the ability to read/send encrypted email and ensures virus control for mobile devices.

#7 Business Associates, Suppliers, Vendors, and Partners: Strong policy and procedures are needed to ensure that all BAs are reviewed for security and privacy practices at least annually. The review should include the inherent risks, financial/business profile risks, and evaluation of security controls.

#8 Cloud Providers: Policy and procedures should be established to manage the full lifecycle of the cloud provider relationship including a contract to provide sufficient security controls, the ability to meet legal and regulatory requirements, and the ability to exit at the end of the contract.

#9 Virtual Physician's Office: Policy, procedures, and technology need to be implemented to protect the PHI data while being gathered from the patient, in transit from the patient location, and during its dissemination to other ecosystem stakeholders.

#10 Wireless Health Care Device Technology: Procedures and technology need to be implemented to ensure data being transmitted from the health care device cannot be compromised during transmission.

#11 State-Sponsored Cyber Crime: Technologies and procedures are needed that can counter the sophisticated attacks of state-sponsored attacks. Many of the same technologies from #3 Outsider Threat can be used in combination with a higher level of expertise to prevent and/or detect these attacks.

In order to secure PHI, an organization's IT department must have documented and implemented procedures and technology in place. While the importance of training cannot be overstated, consider the following list when assessing the current status of security in an organization:

- Risk management (risk identification, threat analysis, etc.)
- Asset management (physical and information)
- Identity management (user IDs, passwords, etc.)
- Physical security (premises protection, visitors, etc.)
- Vulnerability management (secure configuration, patches, etc.)
- Operations management (logs, laptops, desktops, change management, network, mobile devices, removable media, etc.)
- Information protection (encryption, key management, etc.)
- Applications development (code review, testing)
- Threat management (intrusion detection, incident response, etc.)
- Security control testing (penetrations testing, audits, etc.)
- Business continuity (impact analysis, backups, disaster recovery, pandemic planning)

CHAPTER SIX

Survey Findings on Current Practices and Attitudes

In today's health care environment, information technology has the potential to lower health care spending and to improve the efficiency, quality, and safety of medical care delivery.[82]

Using electronic health records will reduce paper work and administrative burdens, cut costs, reduce medical errors, and, most importantly, improve the quality of medical care.[83] However, the risk of data breaches increases with the widespread adoption of EHRs and access to digital health information.[84]

Privacy and security controls developed in the era of paper PHI are now outdated, and organizations that are connected in the expanding health care ecosystem need to work together to ensure the protection of shared data.[85]

So with threats, vulnerabilities, and potential safeguards identified, and security and privacy requirements for protecting PHI mandated, how are organizations responding with their compliance programs?

According to a January 2012 survey of compliance professionals, only 27% felt that they have enough resources for their compliance programs.

Although almost 60% of respondents in the November 2011 Healthcare Information and Management Systems Society (HIMSS) Security Survey indicated that their IT budget dedicated to information security had increased in the past year, 53% admitted that the total allocated to information security was 3% or less of their operational budgets.[86]

And according to a January 2012 survey of compliance professionals, only 27% of the over 970 participants felt that they have enough resources for their compliance programs. Complicating the situation, those same respondents indicated that their greatest cause of stress was "keeping up with new laws and regulations."[87]

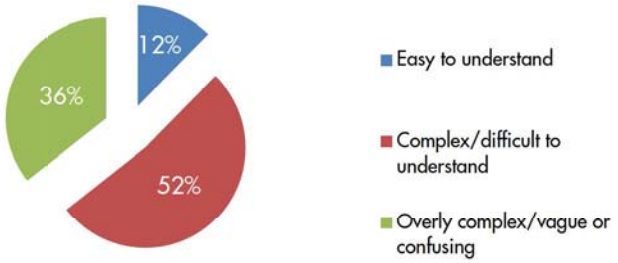
To provide an understanding of industry reaction to federal and state laws, current levels of compliance, and barriers to strengthening compliance programs, in addition to the frequency and ramification of PHI breaches, a survey on PHI was circulated to more than two hundred PHI project participants and to other subject matter experts involved in the protection of PHI. The findings from responses of over 100 qualified participants revealed somewhat conflicting insights as to the effectiveness and management support of current privacy programs.[88]

- 75% "agreed" or "strongly agreed" with the statement "We have effective policies to protect PHI," and
- 76% "agreed" or "strongly agreed" with the statement "We take effective steps to comply";
- ***But*** almost 40% could not agree with the statement that "Management views privacy and security as a priority," and
- 54% could not agree with the statement "We possess sufficient resources to ensure requirements are currently being met."

In the same survey, when asked about the complexity of the laws and the ease of compliance, only 12% felt that they were "easy to understand" and only 14% thought the laws were "not difficult at all" to comply with. Three respondents made the following comments about the laws and regulations:

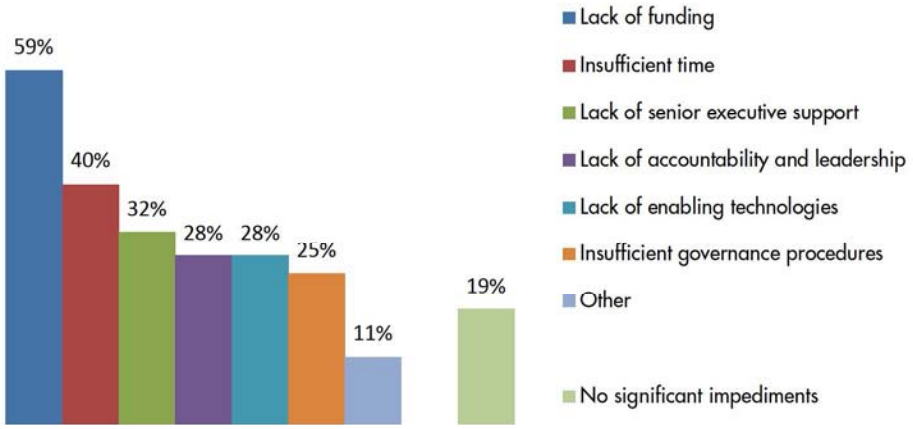
- "There is so much overlap between laws that analysis is time consuming and difficult."
- "We do not have the employee resources or the funds to deal with additional federal regulations."
- "The laws have been ever changing which makes it difficult to keep pace with policies/procedures and training of employees. The process for passage often is annoying because sometimes facilities are expected to comply with the law before it is final."

How would you characterize the complexity of these laws?



How easy is it for your organization to comply with these laws?

When asked to identify the most significant impediments their organization faces to achieving a strong privacy and data security posture with respect to how PHI is collected, used, and retained (multiple answers possible), 59% cited "lack of funding" and 40% indicated "insufficient time." Almost a third (32%) answered "lack of senior executive support," and 28% listed "lack of accountability and leadership."



Although some of the responses indicated that senior management was aware of the great need for security, respondents also indicated that they experienced a lack of senior executive support, and the absence of accountability and leadership in implementing compliance.

One participant stated, "Health care information security is behind the times. Senior leaders need to understand that legacy protection mechanisms like firewalls are no longer adequate."

PHI Security Threats

In response to questions regarding the most likely current threats affecting their organization's ability to secure PHI, a combined 85% stated that the accidental or inadvertent exposure from an insider was the "most likely" or a "very likely" threat. 56% believed that it is "very likely" or "likely" that the organization's current threat comes from malicious insiders.

In addition, malware infestation proved to be a great concern for the organizations participating, with 76% seeing this as a "very likely" or "likely" threat. A combined 61% of respondents felt that their organization is "very likely" or "likely" to fall prey to social engineering attacks. More than 50% of respondents believed that some type of security threat was "likely" affecting their organization in an adverse manner now.

A follow-up question asked respondents to indicate whether they believe these threats will worsen within the next three years; 43% thought that state-sponsored attacks would pose a future threat and 55% indicated that it would be "very likely" or "likely" that future attacks may be perpetrated by malicious insiders. A combined 70% of respondents were concerned that security will be compromised by accidental or inadvertent exposure from an insider.

PHI Breaches and the Financial Impact

When asked whether their organization had experienced a data breach in the last twelve months, only 46% responded definitively that their organization had not suffered a data breach.

In response to questions regarding the financial losses suffered by their organizations due to breaches, only 22% of respondents provided an estimate. Those that provided an estimate stated that their costs were for credit or identity theft monitoring, and for forensic and legal fees. A few respondents mentioned losses due to reputational harm, including loss of goodwill and of business. Another mentioned increased insurance cost. The range of total costs by a handful of respondents who provided estimates was between $8,000 and $300,000.

The survey responses revealed that the majority of participants want to comply and secure PHI, but they believe that budgetary constraints and the lack of executive commitment, leadership, and accountability, as well as the evolving nature of threats and the technologies available to protect PHI, combine to make real protection of health information very challenging.

The full results of the survey are available in Appendix E – Complete Results of Survey: Current Practices and Attitudes.

CHAPTER SEVEN

PHIve – The 5-Step Method of Data Breach Costing

How much should an organization be willing to invest to reduce its risk exposure while gaining a business advantage? An organization that has not suffered a data breach in the last two years is in the minority.[89] The threats to the security of PHI are real, and the incentives for stealing it are financially rewarding.

In addition to the legal and ethical obligations to protect PHI, there is another, very real and equally important reason for protecting it. It is called "goodwill" – the intangible advantages that a company has in its market, including strategic locations, business connections, and, relevant to this matter, an excellent reputation.

Statements prepared under generally accepted accounting principles (GAAP) do not record these "assets," but an organization's reputation for PHI protection is, without a doubt, a market advantage and key to the generation of revenue, the retention of customers, and the productivity of the workforce.

Respondents to the previously cited Ponemon survey believe data breaches suffered by their organizations had resulted in time and productivity loss (81%), in diminished brand or reputation (78%), and in loss of patient goodwill (75%).[90]

So, how much should an organization invest to maintain, if not increase, the value of their goodwill?

This chapter describes **PHIve** – PHI Value Estimator, pronounced five – a 5-step method for PHI protectors to calculate the potential (or actual) cost of a data breach to their organization.

With this ammunition in hand, PHI protectors can determine and recommend the appropriate investments necessary to mitigate the risk of a data breach, thereby reducing potential financial exposure while strengthening their reputation as a protector of the PHI entrusted to their care.

Table 3: PHIve – the 5-Step Method for Calculating the Potential Cost of a Data Breach	
1	Conduct a risk assessment: assess the risks, vulnerabilities, and applicable safeguards for each "PHI home."
2	Determine a "security readiness score" for each "PHI home" by determining the likelihood of a data breach based on the "security readiness score" scale.
3	For each "PHI home" that has an unacceptable "security readiness score," examine the relevance (i.e., likelihood or applicability) of a particular cost category, and apply a "relevance factor" from the relevance factor hierarchy.
4	Determine the impact: relevance x consequence = impact. ■ Relevance – determine the "relevance factor" associated with the cost category for your organization ■ Consequence – calculate the potential cost of the cost category based on considerations for your organization ■ Impact – multiply the "relevance factor" the "consequence" to determine the "adjusted cost"
5	Add up all adjusted costs to determine the total adjusted cost of a data breach to the organization.

Step 1: Conduct a Risk Assessment – Assess the Risks, Vulnerabilities, and Applicable Safeguards for Each "PHI Home"

A "PHI home" is any organizational function or space (administrative, physical, or technical) and/or any application, network, database, or system (electronic) that creates, maintains, stores, transmits, or disposes of ePHI or PHI.

Step 1 involves making a list of every "PHI home" in the organization and in the organizations of any business associates. Assess the potential risk events, vulnerabilities, and applicable safeguards for each organizational function (see examples in Table 4: Determining the Likelihood of Administrative, Physical, and Technical Data Breaches) and for each system/application/database (see examples in Table 5: Determining the Likelihood of Electronic Security Data Breaches).

Table 4: Determining the Likelihood of Administrative, Physical, and Technical Data Breaches

Potential Risk Event	Functional Areas or Responsibilities to Be Considered	Vulnerabilities to Be Considered	Safeguards/Controls to Be Rated
- Physical penetration - Physical destruction - Sabotage - Theft - Unauthorized deletion - Vandalism - Employee error - Information disclosure (e.g., shoulder surfing, elevator chat, wrong recipient) - Improper training of staff - Unavailability of data - Fraud	- Reception - Clinical treatment areas - Data record storage - IT support - Data disposal - Accounting - Billing department - Audit department - Process excellence - Accreditation - Quality outcomes - Human resources - Operations reporting - Facilities	- Physical theft - Intentional or unintentional fax to unauthorized user - Intentional or unintentional email to unauthorized user - Unsecured email - Improper disposal of written documents - Unauthorized creation or modification of written documents - Unauthorized use of written documents - Unauthorized sharing of written documents - Mistaken identity - Untrained or improperly trained workforce member - Failure to establish or update clearance level of workforce member	- New hire background checks - Assigned security responsibility - Documented and enforced policies and procedures - Workforce access authorization clearance processes - Regular workforce training - Sanctions for non-compliance with policies and procedures - Log-in and password management - Incident reporting - Secure facility access - Workstation security and privacy - Business associates' contracts and audits - Regular monitoring and/or auditing of procedures

Table 5: Determining the Likelihood of Electronic Security Data Breaches			
Potential Risk Event	**Applications to Be Considered**	**Vulnerabilities to Be Considered**	**Safeguards/Controls to Be Rated**
- Computer-based attack - Electronic penetration - Destruction of files - Destruction of systems - Sabotage - Theft of ePHI data - Unauthorized creation of ePHI - Unauthorized deletion of ePHI - Unauthorized modification of ePHI - Vandalism	- Admit, discharge, and transfer (ADT) - Medication administration record system (MARS) - Order entry (CPOE) systems or applications - Imaging (PACS) systems or applications - Accounting systems or applications - Billing and receivables systems or applications - Electronic record systems or applications - Dictation and transcription systems or applications - Systems or applications used for utilization reviews - Systems or applications used for accreditation - Systems or applications used for oversight/root cause analysis/governance purposes - Systems or applications used for auditing, credentialing, litigation	- Lack of encryption/decryption capabilities - Lack of reliable data back-up and recovery - Multiple system access - LAN, WAN, or external system pathways - Network pathways - No protection against data interception - No protection against hacking - No protection against port scanning and sniffing - No protection against social engineering - Flaws in technology and software or protocol designs - No protocols for peer-to-peer file sharing - Missing security agents - Unauthorized remote-control software - No controls on media files - Unnecessary modems in laptops - Unauthorized or unsecured synchronization software - No protection against wireless connectivity - No protection against downloading files	- Authentication of authorized users - Strong authentication construction - Documented processes and training - Reviewed and approved clearance for authorized users - Audit controls for identifying unauthorized users - Audit controls for identifying unauthorized activity - Encryption and decryption capabilities - Data integrity controls - Transmission security - Limited to a single system - LAN, WAN, or external system is not protected - No network pathway or unprotected pathway

Step 2: Determine a "Security Readiness Score" for Each "PHI Home" by Determining the Likelihood of a Data Breach Based on the "Security Readiness Score" Scale

Following a full and robust discussion with a cross-functional team of each risk event, vulnerability, and applicable safeguards – strongly recommended to ensure organizational agreement and a unified position when presenting recommendations – assign a "security readiness score" based on the likelihood of a data breach for each PHI home. The previously cited Internet Security Alliance (ISA) and American National Standards Institute (ANSI) joint publications provide a framework for this type of cross-functional team discussion.

While it is certainly up to the organization to determine its risk appetite, one might view a "security readiness score" of 1 or 2 to be acceptable and a score of 4 or 5 to be unacceptable.

Table 6: "Security Readiness Score" Scale

Score	The Likelihood of a Data Breach
1	Virtually impossible
2	Rare
3	Possible but not likely
4	Possible and likely
5	Possible and highly likely

Step 3: For Each "PHI home" That Has an Unacceptable "Security Readiness Score," Examine the Relevance (i.e., Likelihood or Applicability) of a Particular Cost Category, and Apply a "Relevance Factor" from the Relevance Factor Hierarchy

Fines and penalties assessed by the federal and state governments are not the only costs that are included in this calculation. A study found that the organizational costs of data breaches from 2005 to 2010 have exceeded $150 billion, excluding the actual losses sustained by the victims of these breaches.[91]

The cost associated with mitigating an incident after the fact, such as notifying privacy breach victims, providing credit or identity monitoring services to affected individuals, consulting with a public relations firm and/or an investor relations firm to control reputational damage, as well as defense and settlement expenses, can be enormous.[92] Add to this the costs of the resulting business distraction and the declining value of goodwill and the implications are substantial.

Potential data breach repercussions are broken down into five cost categories: (1) reputational, (2) financial, (3) legal/regulatory, (4) operational, and (5) clinical, which have been further broken down into cost impact categories on the following pages.

Relevance

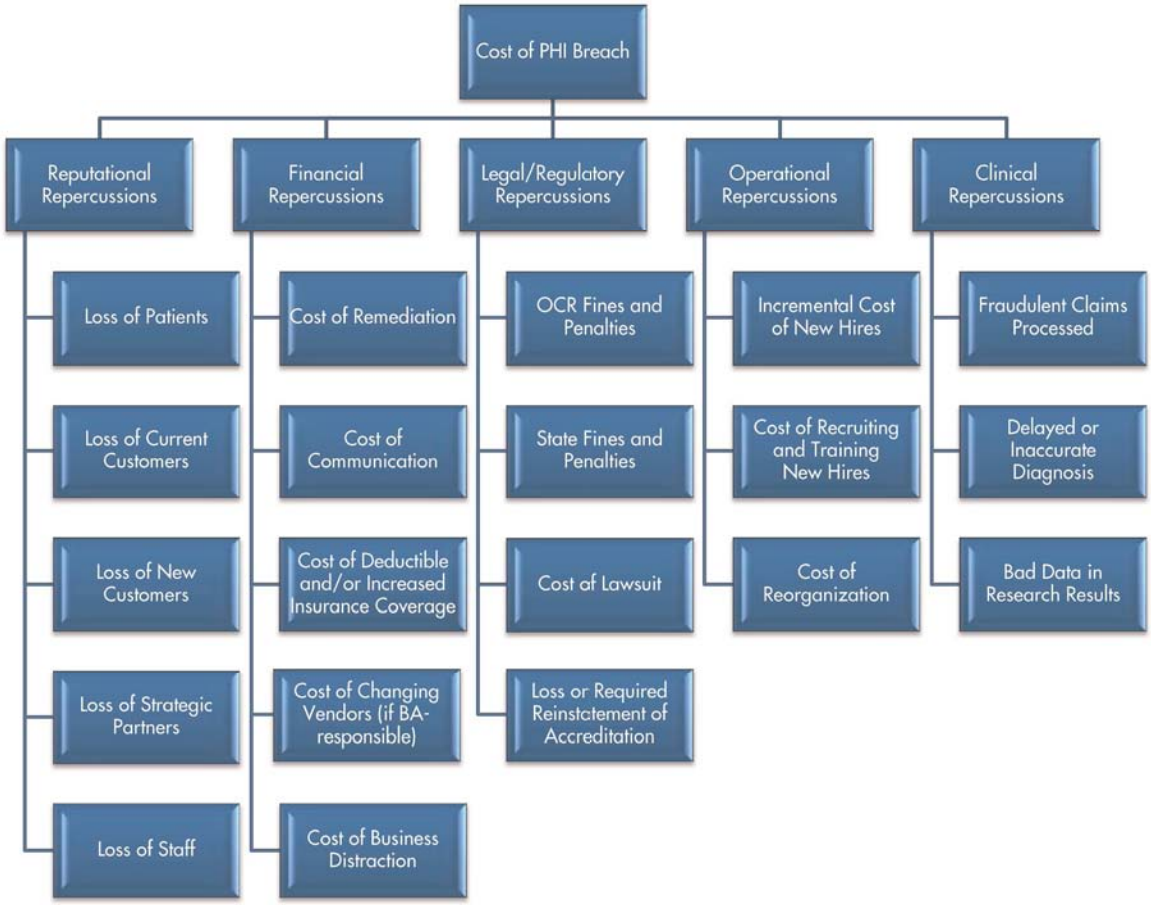
There will be cost categories that may not be relevant to one entity but are extremely relevant to another. For example, when considering the possible repercussions of reputational damage, the work of the organization is critical to the relevancy and level of impact for those specific cost categories. A lab imaging company may not suffer as severe a reputational impact as a single-physician practice. The financial impact of a data breach suffered by a fulfillment company may not be as severe as that suffered by a hospital.

Hard versus Soft Costs

Some cost categories will be easier to calculate or estimate than others. The more challenging categories will take some time for the team to assess and quantify. Prepare for spirited discussions with the cross-functional team charged with managing this issue.

Business Associates

The HIPAA Privacy Rule protects individuals' health information by regulating the circumstances under which covered entities may use and disclose PHI, and by requiring covered entities to have safeguards in place to protect the privacy of the information. As part of these protections, covered entities must have contracts or other arrangements in place with business associates that require access to PHI.[93]



Considerations

Some considerations are provided on the following pages to help stimulate discussions when determining the relevancy and also the potential impact of a particular cost.

When considering the cost categories for each PHI home, assign a relevance factor associated with the likelihood of that cost being incurred if a data breach occurred in that PHI home.

Table 7: Relevance Factor Hierarchy

Relevance	Relevance Factor	Risk Exposure/ Analysis Best Practice
Hardly relevant	0.05	Pre-breach
A little relevant	0.15	
Somewhat relevant	0.50	
Relevant	0.85	
Highly relevant	0.95	
Breach	1.00	Post-breach

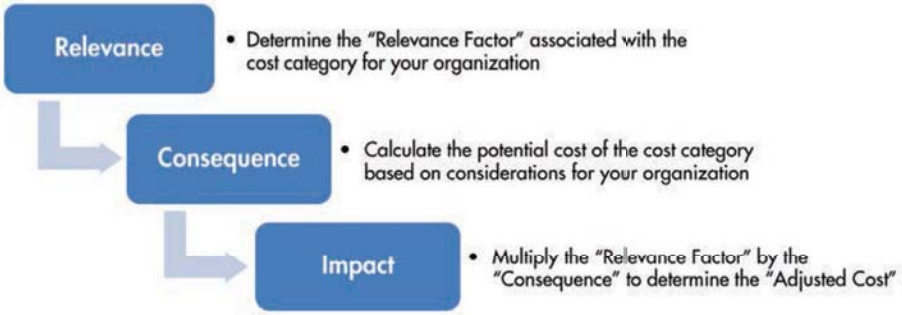
CHAPTER EIGHT

Calculating the Costs of a PHI Breach Using PHIve

PHI is not just "digital data." Each file holds the personal history of an individual and, as such, represents a bond of trust between the individual and the organization entrusted with their data. An organization's ability to maintain that trust is vital to its brand image, reputation, financial success, and longevity.

Therefore, it is not only the hard incremental costs associated with a breach that need to be considered, but also the costs that arise from the impairment of these intangible assets. This should inform your organization's cost calculations in the following categories: reputational, financial, legal/regulatory, operational, and clinical.

Step 4: Determine the Impact: Relevance x Consequence = Impact



This structure largely mimics the common risk assessment formula: **"likelihood" x "consequence" = "impact,"** where "likelihood" has been changed to "relevance" for use in a "cost category."

Using the five repercussion categories suggested below, and the following tips regarding the relevance and impact considerations listed in the tables for each, calculate the relevant adjusted cost of a data breach for each PHI home that has an unacceptable security readiness score.

A. Reputational Repercussions

Table 8: Relevance and Impact Considerations for Reputational Repercussions

Relevance Considerations	Impact Considerations
■ Type of business (CE vs. BA) ■ Availability and acceptability of competitive alternatives	■ Size of breach (>500 records?) ■ Likelihood of harm – Type of data – Age of affected individuals – Income of affected individuals

* "Loss of patients" refers to the individuals who are seeking care (would not typically apply to a BA).

** "Loss of customers" refers to the payer of the services (e.g., for a CE, a health plan may be a customer of a hospital; for a BA, the customer might be a CE. The BA may have more than one CE customer; a subcontractor may have multiple BA customers).

*** Patient churn is the potential result of diminished brand or reputation in combination with the loss of patient goodwill, according to the previously referenced 2011 Ponemon study. The average lifetime value of one lost patient (customer) increased over 5% in the past year.[94]

The Effect of Viral Communications

Consider the story of a lead singer of a Canadian band who posted a music video on YouTube after his guitar was severely damaged by airport baggage handlers. Within three days, it had been viewed close to three-quarters of a million times.[95]

Demographics Matter

In a September 2011 study measuring health privacy sensitivity among certain demographics, consumers rated their sensitivity to 14 health data elements on a 1 to 10 scale. Those in the "46 to 65" age group ranked the highest in privacy sensitivity over their younger and older counterparts; likewise those with the highest income.[96]

Suggested Formulas

- Loss of patients = average revenue per patient x estimated # who would switch to a competitor x a viral factor
- Loss of current customers = average revenue or margin per customer (as appropriate) x # of customers that might switch to a competitor

- Loss of new customers = projected # of new customers discounted for an estimated # who might switch to a competitor x average revenue or margin per customer
- Loss of strategic partners = projected margin per partner x estimated # that would switch to a competitor + cost of identifying and transitioning to new partners
- Loss of staff = average cost of recruiting and training new staff x estimated # of new staff needed as a result of staff losses + (where applicable) average margin not being generated during transition

B. Financial Repercussions

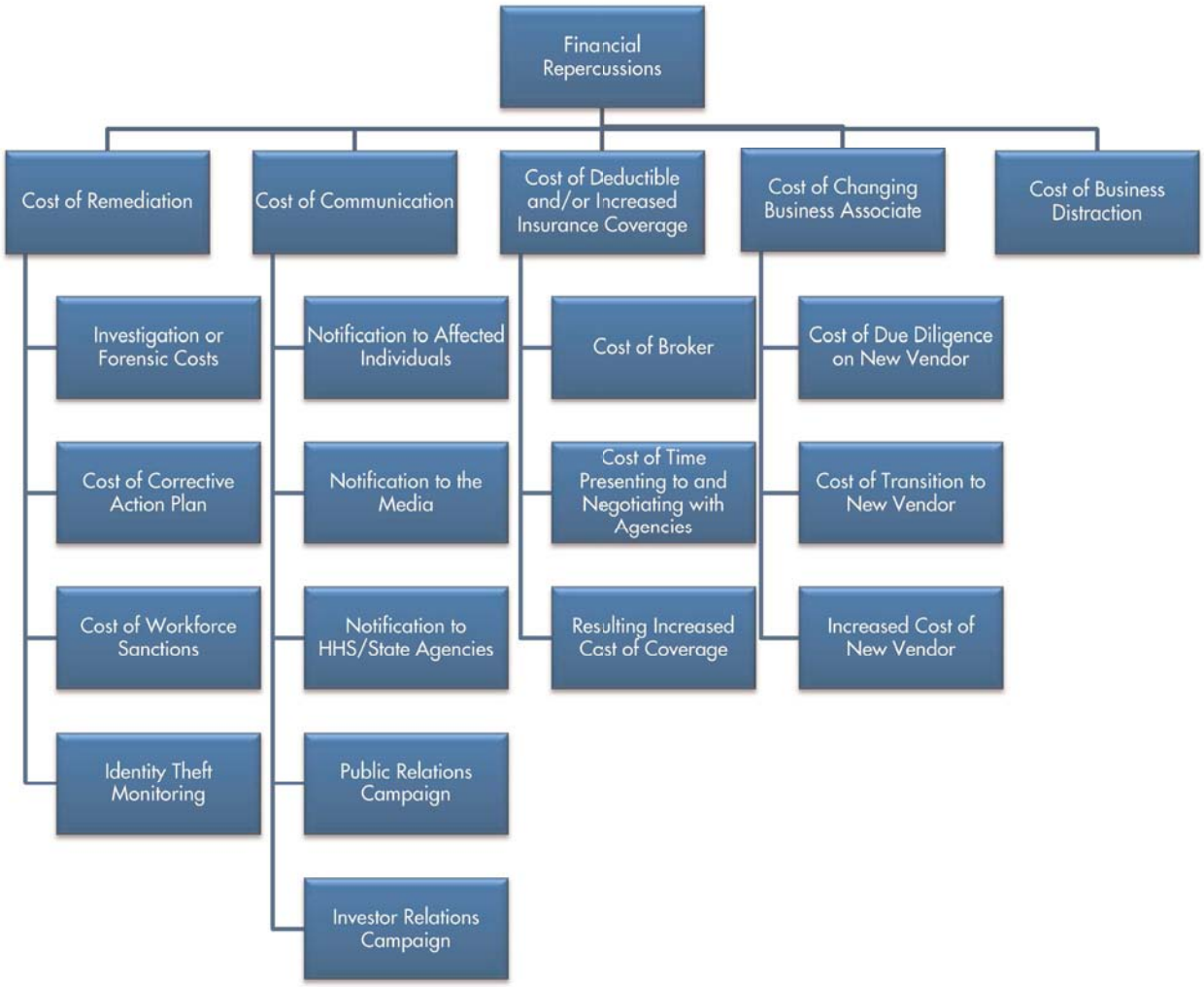


Table 9: Relevance and Impact Considerations for Financial Repercussions	
Relevance Considerations	**Impact Considerations**
■ Size of breach ■ Complexity of breach ■ Strength of safeguards ■ Type of data ■ Breached party (CE or BA) ■ Type of company (public vs. private)	■ Size of breach (>500 records?) ■ Type of breach (malicious vs. unintentional) ■ Likelihood of harm – Type of data – Age of affected individuals – Income of affected individuals

Some considerations to help with this costing:

- **Discovery, Notification, and Response Costs**: The costs following a breach have been estimated by Forrester Research to average about $50 per record.[97]

- **ID Theft Monitoring**: 29% of the respondents in the 2011 Ponemon survey whose organizations had suffered a data breach reported that their data breaches led to cases of identity theft, a 26% increase from the prior year.[98]
  - When the U.S. Department of Veterans Affairs discovers a loss, theft, or exposure, it routinely offers identity theft protection at an average cost per covered individual of $29.95 a year.[99]
  - Industry experts estimate that approximately 20% of affected individuals will actually register for ID theft monitoring services.

- **Size of the Data Breach**: Although a company is required to notify HHS of any and all data breaches on an annual basis, breaches involving the records of 500 or more individuals involve significantly more effort, resources, and cost. Notifications to the following are required within specified timeframes:
  - affected individuals,
  - the media,
  - the secretary of HHS, and
  - the attorneys general in the affected states.[100]

- **Investor Relations Campaign**: Following the recent announcement of a data breach, Sony's stock dropped 2.3% at the close of trading in Tokyo, which some analysts suggest was the result of a legal and political backlash over Sony's delay in notifying affected individuals. The long-term effect of the data breach on the stock price will not be known for a while.[101]

- **Insurance**: At one financial insurer, health care represents about 25% of the data breach insurance business written, but 60% of all claims.[102]

- **Business Distraction**: Although difficult to calculate, the distraction caused by a breach has a real cost in lost productivity. A Forrester report determined that the cost per breached financial record averages about $30 per record for time diverted from other tasks to deal with bad press and legal responsibilities.[103]

C. Legal/Regulatory Repercussions

- **Cost of a Corrective Action Plan (CAP)**: Whether a result of an audit on behalf of HHS, or an internal risk assessment, corrective action plans can be expensive. For a data breach reported by the regents of the University of California, the resolutions with HHS[104] called for a 3-year CAP that included:
  - a complete review, revision, and implementation of policies and procedures;
  - training and monitoring of the workforce;
  - documentation and implementation of sanctions for non-compliance;
  - establishment of a monitor position and monthly reporting requirements on CAP progress;
  - implementation of annual reports on status; and
  - a resolution fee of $865,000.[105]

- **Class Action Lawsuits**: In late 2011, lawyers began closing in on a fixed price of $1,000 per affected individual:
  - Class action lawsuits have been filed against the State of Texas for the posting of unencrypted data on possibly 3.5 million state employees, including one that seeks a $1,000 penalty for each individual affected.[106]
  - In September 2011, Stanford Hospital & Clinic was hit with a $20 million lawsuit for exposing the PHI of some 20,000 patients ($1,000 per patient).[107]
  - A class action lawsuit was filed against the U.S. Department of Defense on October 10, 2011, seeking $1,000 in damages for each of the 4.9 million TRICARE beneficiaries whose records were on a computer tape that was stolen from the car of a government contractor.[108]

While recent cases have used the $1,000 per patient metric, the matter is by no means settled. The ultimate cost to the victim and those liable to the victim will continue to be a moving target, since once ePHI is breached, it is nearly impossible to prevent future misuses of the information and potential harm to the victim.

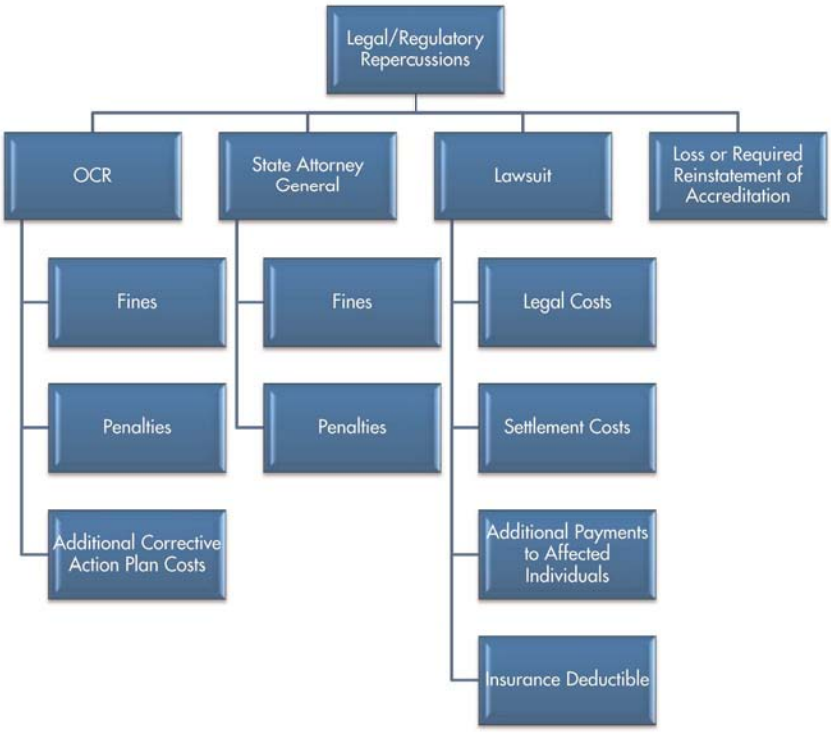


Table 10: Relevance and Impact Considerations for Legal/Regulatory Repercussions	
Relevance Considerations	**Impact Considerations**
■ Type of business (public vs. private) ■ Size of breach ■ Strength of compliance program and culture ■ Number of previous breaches ■ Type of data ■ Breached party (CE or BA)	■ Size of breach (>500 records?) ■ Type of breach (malicious vs. unintentional) ■ Likelihood of harm – Type of data – Age of affected individuals – Income of affected individuals ■ Resident state of affected individuals

- **Location of Affected Individuals**: Currently 46 states have data breach notification laws and the state attorneys general are enforcing them to protect their residents and gain significant settlements. Texas expanded the notification requirements to cover affected non-residents and is imposing further notification requirements for a breach of health information.[109] Although Health Net fully cooperated, provided two years of credit monitoring services, and improved data and equipment security, the Connecticut Insurance Department fined the health insurer $375,000 for the lack of timely notification following a large breach of personal health information in late 2009.[110]

- **State Contract and Tort Law**: In addition to professional enforcement by licensing boards, state tort law and contractual theories may be available to provide redress for individuals whose health information may not have been collected, used, processed, or disclosed appropriately. While the types of actions that may apply are far too numerous to digest in detail, state tort and/or contract or quasi-contract theories for unauthorized disclosure of health information may include the following: (i) negligence; (ii) intentional and/or negligent infliction of emotional distress; (iii) breach of fiduciary duty; (iv) professional malpractice; (v) unjust enrichment; (vi) invasion of privacy; (vii) intrusion upon seclusion; (viii) false light in the public eye; (ix) violation of rights of publicity; (x) defamation; (xi) breach of confidence; (xii) breach of contract implied and/or express; (xiii) harassment; (xiv) prima facie tort; and, (xv) other theories adopting private causes of action from state statute or constitutional law (such as patient Bill of Rights–type theories). These laws apply broadly, since traditional and non-traditional tort theories may apply. Outside of any alleged mental anguish–type damages, if one does not suffer actual monetary damages, the reach of state tort law to provide redress is somewhat of an open issue. However, there are new damages theories that are being advanced based upon the value of the information to an individual. When actual out-of-pocket damages are suffered (for example, where one expends time and/or money to repair their health information records after medical identity theft), tort law may provide retribution to the affected individuals.

- **Criminal Penalties**: HIPAA, as amended by the HITECH Act, provides for criminal penalties for knowingly, and in violation of the law, using or causing to be used a unique health identifier, obtaining individually identifiable health information relating to an individual, or disclosing individually identifiable health information to another person. Those penalties range from $50,000 to $250,000 and/or one to ten years in prison.[111]

- **Civil Penalties**: Civil monetary penalties are also available and were increased to a maximum of $25,000 to $1.5 million depending on whether the person or entity violating the law exercised "reasonable diligence" or the violation was due to "willful neglect."[112] The secretary of HHS is required to impose a penalty for all violations due to "willful neglect," defined as "conscious, intentional failure or reckless indifference" to the obligation owed an individual.[113] Failing to comply with requirements of the HIPAA Privacy and Security Rules would likely meet this definition.

- Tier A violations: did not realize and would have handled the matter differently -
  - $100 fine for each affected individual, and
  - $25,000, maximum total imposed for the calendar year.
- Tier B violations: due to reasonable cause, but not "willful neglect" -
  - $1,000 fine for each affected individual, and
  - $100,000, maximum total imposed for the calendar year.
- Tier C violations: due to willful neglect, ultimately corrected -
  - $10,000 fine each affected individual, and
  - $250,000, maximum total imposed for the calendar year.
- Tier D violations: willful neglect, uncorrected -
  - $50,000 fine for each affected individual, and
  - $1,500,000, maximum total imposed for the calendar year.

- The HITECH Act authorizes state attorneys general to bring lawsuits against individuals and organizations on behalf of residents for violations of any provisions of the HIPAA and HITECH laws and may recover damages of $100 per violation up to $25,000 in a calendar year, plus attorney's fees.[114] Some state health privacy laws impose higher monetary penalties on breaching parties, and recently the Indiana attorney general invoked state law, over HIPAA/HITECH, when prosecuting a privacy breach by insurer WellPoint, Inc.[115]

- Finally, the HITECH Act requires the secretary of HHS to establish by 2012 a methodology by which any individual harmed by a violation of the HIPAA or HITECH Acts may recover a percentage of any civil monetary penalty or monetary settlement.[116] This provision is likely to increase the number of complaints that cite violations of the privacy and security laws.

D. Operational Repercussions

Table 11: Relevance and Impact Considerations for Operational Repercussions

Relevance Considerations	Impact Considerations
■ Sufficiency of current resources	■ Number of additional resources needed
■ Appropriateness of placement of compliance program in organizational structure	■ Level of disruption of required organizational changes

In addition to any remediation or corrective action plan (CAP) required by OCR, additional operational costs associated with strengthening a compliance program may be necessary or appropriate following a data breach. These costs might include hiring outside consultants to design and/or deliver a more effective training program or the hiring of additional employees with needed skills, knowledge, and experience, to handle technology security requirements. In some cases, a higher-level employee in the organization may be needed to heighten awareness and strengthen the power of the decisions to be made. Organizational changes often disrupt the organization for a period of time, which comes with a loss of productivity.

E. Clinical Repercussions

The rise of medical identity theft has led to increased costs for the health care industry and the victims. Schemes involve the lending and borrowing of a valid ID to access health care services.[117] Over one third (36%) of provider organizations participating in the PwC survey confirmed that they have experienced patients seeking services using somebody else's name and identification.[118]

Medical identity theft is especially expensive and potentially dangerous for the victim. If medical files have been altered, it can lead to the administration of incorrect care with disastrous results. It can result in the mistaken belief that the victim is ineligible for both life and health insurance. Misdirected and unpaid medical bills can result in damage to credit scores.

The result of these complications is that the average financial damage done to the clinical fraud victim can be as much as $20,000,[119] a cost increasingly being borne by the covered entity as the responsible party for the PHI breach.[120]

In addition, any medical research utilizing inaccurate data from altered medical records to create new evidence-based care could lead to future patients either receiving improper care or having proper care withheld or delayed.

Table 12: Relevance and Impact Considerations for Clinical Repercussions

Relevance Considerations	Impact Considerations
■ Type of data (prescription vs. medical care)	■ Type of data (prescription vs. medical care) ■ Intent (malicious vs. unintentional) ■ Age and income of affected individuals ■ Number of records breached

Step 5: Add up All Adjusted Costs to Determine the Total Adjusted Cost of a Data Breach to the Organization

A number of studies and surveys have provided an average, or estimate, of the total cost of a data breach, and some have turned that total cost into a cost per record breached. But not every data breach is the same, and not every organization that experiences a data breach will incur the same costs. As the previous pages have pointed out, the relevance and impact considerations can drive a wide range of liabilities.

In order to determine a customized cost of a data breach to your organization, total up all adjusted costs for all PHI homes that have an unacceptable security readiness score to determine a total adjusted cost of a data breach to your organization. Compare that total adjusted cost to the table at right to determine the significance level of a data breach to your organization given its current level of threats, risks events, vulnerabilities, and safeguards.

Table 13: Scoring the Total Impact

Insignificant	Less than 2% of revenue
Minor	2% of revenue
Moderate	4% of revenue
Major	6% of revenue
Severe	Greater than 6% of revenue

Armed with this total adjusted cost and the potential total impact of a breach to your organization, in addition to the assessments, security readiness scores, relevance and impact considerations, relevance factors, and adjusted costs, you can determine and recommend a solid rationale for an investment in strengthening your compliance program along with a list of prioritized risk mitigation initiatives.

How Much Should Be Invested to Strengthen a Privacy and Security Program?

To determine a recommended level of investment, a quantitative risk assessment method involves the calculation of the annualized loss expectancy (ALE) of a data breach. Multiply the average cost of one incident (also known as single loss expectancy or SLE) by the probability that the incident will occur during one year (also known as the annualized rate of occurrence or ARO).

$$ALE = SLE \times ARO$$

The SLE in this case is the total adjusted cost calculated above. The ARO will be a much discussed factor for your team, and will be based on the level of safeguards and controls that your organization has in place, your history of breaches and remediation actions, and those of your business associates and subcontractors.

As a reminder, from the 2011 Ponemon study, 96% of the provider organizations studied reported having had at least one data breach in the past 24 months.[121]

An example of the costing of a data breach specific to the hypothetical scenario presented in chapter four is provided on the next pages, including relevance and impact considerations, followed by calculations of those costs based on estimates and statistical studies.

Assuming the probability that the organization in the scenario will incur a breach every two years, the ARO = ½ or 50%, which when multiplied by the SLE of $26,493,617 (total adjusted cost of a breach) results in an ALE of $13,246,809.

If an investment in strengthening the privacy and security program could reduce the probability of a data breach from once every two years to once every five years, the ARO would become 1/5 (or 20%), which when multiplied by the SLE of $26,493,617 results in an ALE of $5,298,723.

The reduction in the ALE from today's exposure of $13.2 million to a potential exposure of $5.3 million supports an investment of $7.9 million in initiatives that can produce that level of reduction in the probability of a breach. (Note: $7.9 million is approximately 3.3% of that organization's annual revenue.)

And, do bear in mind the following: "On average, the breached firms lost 2.1 percent of their market value within two days following the public announcement."[122] The cost of an internally developed corrective action plan is a direct investment in your organization's reputation as a protector of PHI.

Costing of a Scenario: Unintentional, Business Associate, 845,000 Records, Clinical Fraud Resulting in 1 Death, Financial and Clinical Fraud, NY

COST DOMAIN	COST CATEGORY	COST SUB-CATEGORY	RELEVANCE CONSIDERATIONS	IMPACT CONSIDERATIONS	TOTAL COST
REPUTATIONAL	LOSS OF CURRENT PATIENTS/CUSTOMERS		AVAILABLE ALTERNATIVES IN NYC	WOMAN'S WRONGFUL DEATH SEVERELY DAMAGES REPUTATION	$ 8,947,947
	LOSS OF NEW BUSINESS		AVAILABLE ALTERNATIVES IN NYC	WOMAN'S WRONGFUL DEATH SEVERELY DAMAGES REPUTATION	$ 1,934,691
	LOSS OF STAFF		AVAILABLE ALTERNATIVES IN NYC	IMPORTANCE OF REPUTATION; AVAILABILITY AND COST OF PROFESSIONAL STAFF	$ 113,880
FINANCIAL	REMEDIATION	CORRECTIVE ACTION PLAN	MODIFICATION OF DISASTER RECOVERY AND BUSINESS CONTINUITY POLICIES TO INCLUDE HARD DRIVE FAILURES; ESTABLISH AUDIT AND SECURITY VETTING PROCEDURES FOR DATA RECOVERY VENDORS; RECONSTRUCT ALTERED RECORDS	AVAILABILITY OF RESOURCES TO DOCUMENT, IMPLEMENT AND TRAIN ON NEW PROCEDURES, # OF RECORDS ALTERED, COST OF NEW EQUIPMENT	$ 2,452,780
		WORKFORCE SANCTIONS	FIRED CISO AND IT MANAGER	AVAILABILITY OF REPLACEMENT STAFF, COST OF RECRUITING AND REPLACEMENT SALARIES	$ 81,000
		ID THEFT MONITORING	# OF RECORDS; TYPE OF INFORMATION	# OF YEARS PROVIDED	$ 3,430,129
		LOSS OF PRODUCTIVITY	COMPLEXITY OF BREACH	# OF INVOLVED INDIVIDUALS; MAGNITUDE OF CHANGES	$ 48,000
	COMMUNICATION	AFFECTED INDIVIDUALS	SIZE OF BREACH >500 RECORDS	# OF AFFECTED INDIVIDUALS, HHS, MEDIA	$ 1,686,550
		MEDIA	SIZE OF BREACH	DEATH RESULTING FROM BREACH	$ 5,000
		HHS/STATE AG	SIZE OF BREACH	DEATH RESULTING FROM BREACH	$ 5,000
		PUBLIC RELATIONS	SIZE OF BREACH, REPUTATION IN COMMUNITY	USE OF OUTSIDE CONSULTANTS, COST OF ADVERTISING	$ 305,000
	CHANGE IN VENDORS (if BA-RELATED)	DEVELOP RFP, AUDIT SECURITY & HIPAA COMPLIANCE	LEVEL OF PREVIOUS COMPLIANCE	USE OF THIRD-PARTY INDEPENDENT SECURITY AUDITOR	$ 18,000
		TRANSITION TO NEW VENDOR	INCREASED AUDITS TO ENSURE COMPLIANCE	LENGTH OF TRANSITION TIME: DUPLICATE COSTS DURING TRANSITION	$ 5,000
		ADDITIONAL COST ASSOCIATED WITH NEW VENDOR	LEVEL OF PREVIOUS COMPLIANCE	DIFFERENTIAL IN LEVEL OF SECURITY AND HIPAA COMPLIANCE FROM PREVIOUS VENDOR	$ 15,000
LEGAL	OCR	FINES	WRONGFUL DEATH; ACCOUNTABILITY: LACK OF VETTING POLICY AND PROCEDURES FOR VERIFICATION OF SERVICE PROVIDER'S DATA SECURITY PROTOCOLS, PROOF OF COMPLIANCE AND SECURITY CERTIFICATION	HOSPITAL COOPERATED, BUT THE NEGLIGENCE ASSOCIATED WITH VETTING 3RD PARTY VENDOR DETERMINED "WILLFUL NEGLECT"	$ 250,000
	STATE AG	FINES	SIZE OF BREACH	WRONGFUL DEATH	$ 338,000
	LAWSUIT	LEGAL, SETTLEMENT, ADDITIONAL PAYMENTS & INSURANCE DEDUCTIBLE	SIZE OF BREACH, AGE & INCOME OF AFFECTED INDIVIDUALS, MEDICAL & FINANCIAL FRAUD	WRONGFUL DEATH, CREDIT CARD LIABILITIES	$ 5,970,000
	LOSS OF ACCREDITATION	PCI	FINANCIAL FRAUD	RE-ESTABLISH ACCREDITATION	$ 793,000
OPERATIONAL	COSTOF NEW HIRES	BA -RELATED BREACH; NO ADDITIONAL STAFF NEEDED	ADDED STAFF IN REMEDIATION PLAN	# OF ADDITIONAL STAFF REQUIRED FOR COMPLIANCE	$ -
CLINICAL	FRAUDULENT CLAIMS PROCESSED		FRAUD	TYPE OF DATA: PRESCRIPTION" MORE FREQUENT BUT LESS COSTLY VS. FREE MEDICAL CARE: LESS FREQUENT BUT MORE COSTLY	$ 94,640
	GRAND TOTAL COST OF DATA BREACH				**$ 26,493,617**
	TOTAL ANNUAL REVENUE OF CLAIMS PAYER				**$ 241,836,404**
	% OF DATA BREACH COST TO TOTAL ANNUAL REVENUE				**11%**
				IMPACT	**SEVERE**

Scoring the Impact*	
Insignificant	Less than 2% of Revenue
Minor	2% of Revenue
Moderate	4% of revenue
Major	6% of Revenue
Severe	Greater than 6% of Revenue

Cost/Record	$	31.35
Cost/Affected Individual	$	7,838.35
Annualized Lost Excpectancy*	$	5,298,723
*the cost of risk for one year based on the proability that the incident will occur during one year assuming a data breach once every (# years)		5

Calculation of the Annualized Lost Expectancy:

• Single Lost Expectancy (SLE) = the average cost of one incident	$	26,493,617
• Annualized Rate of Occurrence (ARO) = the probability that the incident will occur during one year		0.20
• Annualized Lost Expectancy (ALE) the cost of risk for one year: ALE = SLE * ARO	$	5,298,723

Selected Calculations of Costs Incurred by the Hospital in the Hypothetical Scenario Provided in Chapter 4

(These calculations are based on the details of this hypothetical example; specific analysis for an organization should reflect the relevance and impact for that organization.)

	line #	Our Example	Source
Reputational Repercussions			
Loss of Current Patients:			
Annual Hospital Revenue	1	$241,836,404	This example: from hospital records
# of Patients Records	2	845,000	This example: records breached
% of Active Patients	3	37.5%	This example: % of active patients
# of Active Patients	4	316,875	line 2 * line 3
Revenue/Active Patient	5	$ 763.19	line 1/line 4
Patient churn due to reputational harm	6	3.70%	Ponemon Study: Effect of Customer Churn http://www.ponemon.org/news-2/23
Revenue Loss associated with loss of active patients	7	$ 8,947,947	line 4 * line 5 * line 6
Loss of New Patients:			
Forecast % of new active patients next year	8	10%	This example: from Finance Budgeting assumptions
Expected # of new patients per year	9	31,687.50	line 4 * line 8
Projected new revenue	10	$24,183,640	line 5 * line 9
% revenue loss due to negative publicity	11	8%	This example: 20% reduction in forecast new business (financial estimates of viral impact) and availability of competition
Loss of New Patient Revenue	12	$ 1,934,691	line 10 * line 11
Loss of Stratetic Partners:	13	$ -	all health plans stayed with the hospital
Loss of Staff:			
Recruiting Cost	14	$ 83,880	Replaced one cardiothoraic surgeon who quit and joined competition $419,400 * 20% recruiting fee http://www1.salary.com/Surgeon-Cardiothoracic-Salary.html
Incremental higher salary of new surgeon	15	$ 30,000	higher salary required to entice surgeon due to breach
Loss of Staff	16	$ 113,880	line 14 + line 15
Total Reputation Repercussions	17	$ 10,996,518	Line 7 + line 12 + line 13 + line 16
Financial Repercussions			
Cost of Remediation			
a Investigation and Forensic Costs	18	$ -	this example: used in-house resources
b Cost of Corrective Action Plan			
Cost of Documenting, Implementing & Training New Procedures	19	$ 200,000	this example: outsourced; based on contractor responses to RFP
Cost To Reconstruct Records			
# of records breached	20	845,000	this example: # of records breached
% of records altered	21	0.4%	FBI Fraud Estimate
# of altered records	22	3,380	line 20 * line 21
Cost of Record Reconstruction	23	$ 631.00	https://www.javelinstrategy.com/news/1170/92/1
Total Cost of Rebuilding Records	24	$ 2,132,780	line 22 * line 23
Cost of incremental staff for auditing policies and procedures	25	$ 100,000	this example: one auditor @ $65,000 + 20% benefit rate + laptop, etc.
Cost of new hard drives	26	$ 20,000	this example: replacement of failed hard drive + backup
Total Cost of Corrective Action Plan	27	$ 2,452,780	line 19 + line 24+ line 25 + line 26
c Workforce Sanctions			
Recruiting Cost	28	$ 45,000	20% of annual salaries: $ 125,000 for new CISO; $100,000 for new IT Manager
Incremental Higher Salaries & Benefits	29	$ 36,000	previous salaries were $105,000 for CISO; $90,000 for IT Manager
Total Cost of Workforce Sanctions	30	$ 81,000	line 28 + line 29
d ID Theft Monitoring			
# of records	31	845,000	this example: # of records breached
% of individuals needing Credit Monitoring	32	0.40%	FBI Fraud Estimate; quote by FIT field agent, Tom Liffiton from discussion in InfraGard Meeting at the University of Advancing Technologies
# of individuals needing Credit Monitoring	33	3,380	line 31 * line 32
Cost of Credit Monitoring/affected individual/year	34	$ 31.95	https://www.gsaadvantage.gov/advantage/search/specialCategory.do?cat=ADV.SS&group=0#0
Cost of Credit Monitoring for affected individuals for two years	35	$ 215,982	line 33 * line 34 * 2 years
# of Individuals eligible for Fraud Watch	36	841,620	line 31 - line 33
% of Individuals who will take advantage of Fraud Watch	37	19%	from industry experts
# of Individuals who will take advantage of Fraud Watch	38	159,908	line 36 * line 37
Cost of ID Fraud Watch/non-affected individuals/year	39	$ 10.05	https://www.gsaadvantage.gov/advantage/search/specialCategory.do?cat=ADV.SS&group=0#0
Cost of ID Fraud Watch for non-affected individuals for two years	40	$ 3,214,147	line 38 * line 39 * 2 years
Total Cost of ID Theft Monitoring for two years	41	$ 3,430,129	line 35 + line 40

	line #	Our Example	Source
e Cost of Lost Productivity			
# of months between discovery to remediation resolution	42	6	this example: associated with investigation & organizational changes
% decline in productivity	43	3%	this example: financial estimate
semi-annual payroll for IT personnel	44	$ 1,600,000	this example: 40 staff in IT @ avg annual salary of $80,000 for 6 months
Total Cost of Lost Productivity	45	$ 48,000	line 43 * line 44
Total Cost of Remediation	46	$ 6,011,909	line 18 + line 27 + line 30 + line 41 + line 45
Cost of Communication			
a Notification to Affected Individuals			
Affected Individuals	47	845,000	This example: # of records breached > 500 records
Message Development	48	$ -	This example: in-house content development
Legal Review	49	$ 5,000	This example: finance estimate
Printing Cost	50	$ 0.49	This example: finance estimate
Mailing	51	$ 1.50	This example: finance estimate
Total Notification Cost to Affected Individuals	52	$ 1,686,550	((line 50 + line 51) * line 47) + line 48 + line 49
b Notification to Media			
Message Development	53	$ -	this example: in-house content development
Legal Review	54	$ 5,000	this example: finance estimate
Printing/Mailing Cost	55	$ -	this example: distributed electronically
Total NotificationCosts to Media	56	$ 5,000	line 53 + line 54 + line 55
c Notification to HHS/State Agencies			
Message Development	57	$ -	this example: in-house content development
Legal Review	58	$ 5,000	this example: finance estimate
Printing/Mailing Cost	59	$ -	this example: distributed electronically
Total Notification Costs to HHS/State Agencies	60	$ 5,000	line 57 + line 58 + line 59
d Public Relations Campaign			
Campaign Development	61	$ 100,000	this example: outsourced to Marketing Firm, based on responses to RFP
Legal Review	62	$ 5,000	this example: finance estimate
Advertising in Local Newspapers & Other Media	63	$ 200,000	this example: advertisements in the New York Times and radio spots
Business Distraction of CEO/CFO (interviews)	64	$ -	a real cost but difficult to quantify
Total Public Relations Campaign Cost	65	$ 305,000	line 61 + line 62 + line 63 + line 64
Total Cost of Communication	66	$ 2,001,550	line 52 + line 56 + line 60 + line 65
Cost of Increased Insurance Coverage			
a Broker Fees	67	$ -	This example: not applicable
b Presentation and Negotiation Time	68	$ -	this example: not applicable
c Business Distraction of Financial Resources	69	$ -	this example: not applicable
d Resulting Increased Cost of Coverage	70	$ -	this example: not applicable
Total Cost of Increased Insurance Coverage	71	$ -	this example: not applicable
Cost of Changing Business Associate (Data Backup)			
a Cost of Due Diligence on New Data Back-up Vendor	72	$ 18,000	this example: 3rd party independent privacy and security assessment
b Cost of Transition Time to New Vendor	73	$ 5,000	this example: 60 day duplicate cost
c Increased Annual Cost of New Vendor	74	$ 15,000	this example: higher due to more stringent security policies and procedures
Total Cost of Changing Business Associate	75	$ 38,000	line 72 + line 73 + line 74
Total Financial Repercussions	76	$ 8,051,459	line 46 + line 66 + line 71 + line 75

Legal & Regulatory Repercussions

OCR Fines, Penalties and CAP costs			
a Fines			
# of Altered Records	77	3,380	line 22
Tier C Violation: "due to willfull neglect; ultimately corrected"	78	$ 250,000	this example: $10,000/affected individual up to $250,000 per calendar year
b Penalties	79	$ -	this example: none assessed due to prompt investigation and notification
c Additional Corrective Action Plan costs			
Monthly and Annual reports on progress	80	$ -	this example: responsibilities included with Audit position noted above
Total OCR Fines, Penalties and CAP costs	81	$ 250,000	line 78 + line 79 + line 80
State Fines and Penalties			
a Fines			
# of Altered Records	82	3,380	line 22
NY State AG	83	$ 338,000	this example: $100 fine per affected individual higher due to resulting death
b Penalties	84	$ -	this example: none assessed
Total State Fines & Penalties	85	$ 338,000	line 83 + line 84

	line #		Our Example	Source
Lawsuit				
a Legal Costs	86	$	100,000	this example: settled quickly so minimized legal costs
b Settlement Costs	87	$	3,380,000	this example: $1,000 per affected individual
c Additional Payments to Affected Individuals	88	$	500,000	this example: paid to the family of the woman who died
d Insurance Deductible	89	$	300,000	this example: insurance deductible
e Credit Card Fraudulent Claims Processed				
% of Records Exploited	90		0.40%	FBI Fraud Estimate; quote by FIT field agent, Tom Liffiton from discussion in InfraGard Meeting at the University of Advancing Technologies
Impacted Card holders	91		3,380	line 90 * line 2
Average Loss per Card	92		$500.00	http://www.whitecanyon.com/identity-theft-statistics.php
Total Fraudulent Claims Processed	93	$	1,690,000	line 91 * line 92
Total Lawsuit Costs	94	$	5,970,000	line 86 + line 87 + line 88 + line 89 + line 93
Reinstatement of Accreditation	95	$	793,000	http://www.braintreepayments.com/blog/what-does-it-cost-to-become-pci-compliant
Total Legal and Regulatory Repercussions	96	$	7,351,000	line 81 + line 85 + line 94 + line 95
Operational Repercussions				
Incremental Cost of New Hires	97	$	-	this example: since Business Associate issue, no additional from above
Cost of Recruiting & Training New Hires	98	$	-	this example: since Business Associate issue, no additional from above
Cost of Reorganization	99	$	-	this example: since Business Associate issue, no additional from above
Total Operational Repercussions	100	$	-	line 97 + line 98 + line 99
Clinical Repercussions				
Fraudulent Claims Processed				
# of Affected Individuals of ID Theft	101		3,380	line 32
% related to Medical Fraudulent Claims Processed	102		0.40%	FBI Fraud Estimate
# of Medical Fraudulent Claims Processed	103		14	line 101 * line 102
Average cost per claim	104		$7,000	http://www.ahipresearch.org/pdfs/FraudPrevention2011.pdf
Total Cost of Fraudulent Medical Claims Processed	105		$94,640	line 103 * line 104
Delayed or Inaccurate Diagnosis	106	$	-	this example: none identified
Total Clincial Repercussions	107	$	94,640	line 105 + line 106
Total Impact of Data Breach	**108**	**$**	**26,493,617**	line 17 + line 76 + line 96 + line 100 + line 107
			-	

FINALE

The health care ecosystem is trying to keep in step with today's technology, reflected in its move to adopt electronic health records.

However, in the course of making this dramatic change to the way health care data is created, stored, and transmitted, the safeguarding of protected health information is not always given top priority.

With the increase in nefarious intent as well as the rewards and opportunities to steal PHI, the likelihood of a data breach for most organizations is very high.

> **No organization can afford to ignore the potential consequences of a data breach.**

Recognize the Risks

To successfully mitigate data breach threats and risks, leaders of organizations in the health care sector must understand the evolving health care ecosystem, and the role that their organization and their subcontractors play in it.

They need to ensure that their organization complies with evolving federal and state health care regulations, and they must understand that non-compliance may result in fines and civil penalties, imposed on both the organization and its leaders.

And they should be aware that, in the future, non-compliance may rise to the level of a criminal offense.

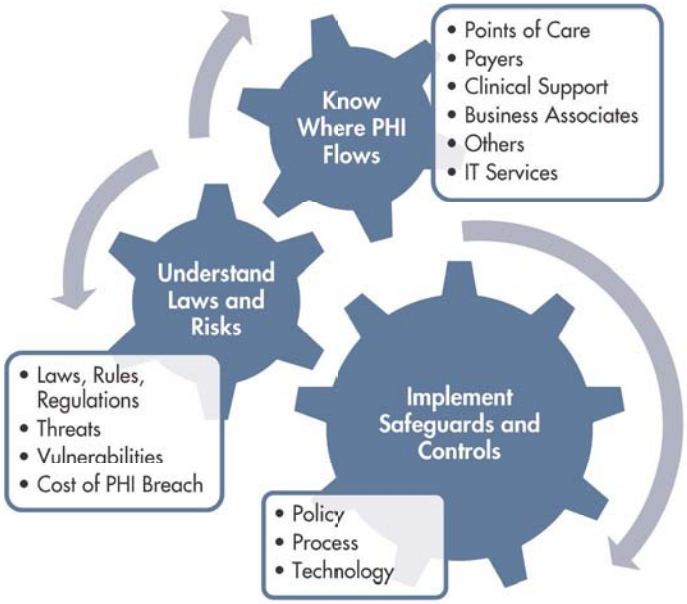
But these are not the only costs and concerns facing organizational leaders. The repercussions of a data breach can be very high and long-lasting – lost business due to reputational harm; penalties, fines, and corrective action plans assessed by HHS and state attorneys general; and the business distraction and impact of increasing class action suits, legal costs, and settlements.

Implement Safeguards and Controls

Organizations entrusted with the protection of PHI need to have a comprehensive understanding of where their PHI is stored, and how it is shared with third parties. All internal and external information flows, as well as threats and vulnerabilities, should be assessed. A sound analysis of the likelihood and impact of a data breach should be undertaken using PHIve, the 5-step method described in this report.

Preventing or detecting a breach requires that effective policies, procedures, and technologies are in place. It is important to gain executive support and develop a good business plan to secure sufficient resources for execution. While it is impossible to eliminate all risks, many can be mitigated in order to reduce significantly the likelihood and impact of a breach, and to ensure that ethical and legal requirements are met. Recommendations for prioritized investments in an enhanced security program, resulting from conducting an organizational risk assessment, can be paid for by the reduced likelihood of a breach.

Those who follow this approach will improve their organization's security posture as well as its bottom line. They also deserve a gracious "thank you" from all the people who trust them to protect their most personal health information.



ENDNOTES

[1] Hsiao, Chun-Ju, et al. "Electronic Medical Record/ Electronic Health Record Use by Office-based Physicians: United States, 2008 and Preliminary 2009." Rep. National Center for Health Statistics, Dec. 2009. Web. http://www.cdc.gov/nchs/data/hestat/emr_ehr/emr_ehr.htm.

[2] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[3] HHS Finding, 65 Fed. Reg. at 82,465; "An Ominous Milestone: 100 Million Data Leaks," The New York Times, Dec. 18, 2006; "Vast Data Cache About Veterans is Stolen," The New York Times, May 23, 2006; "Veterans Administration Loses Data," Consumer Affairs, Feb. 18, 2007; "Medicare and Medicaid Gaps Are Found," The New York Times, Oct. 21, 2006.

[4] "Experts: Medical Identity Theft Growing, Tough to Detect," Philadelphia Business Journal, Oct. 19, 2007; "Breaking the Code: How Credit-Card Data Went Out Wireless Door," Wall Street Journal, May 4, 2007; "Medical Identity Theft Is a Growing Problem," The Heartland Institute, Sept. 2007.

[5] HHS Finding, 65 Fed. Reg. at 82,465.

[6] Executive Office of the President of the United States. "National Strategy for Trusted Identities in Cyberspace." Apr. 15, 2011. Web. http://www.whitehouse.gov/blog/2011/04/15/president-obama-releases-national-strategy-trusted-identities-cyberspace.

[7] Id. at p. 6.

[8] Anderson, Howard. "Congress Probes TRICARE Breach." GovInfoSecurity.com. GovInfo Security, Dec. 2, 2011. Web. http://www.govinfosecurity.com/articles.php?art_id=4299.

[9] Abelson, Reed, and Katie Thomas. "Cuts in Health Care May Undermine Role in Labor Market." The New York Times, Aug. 17, 2011. Web. http://www.nytimes.com/2011/08/18/business/cuts-in-health-care-may-undermine-role-in-labor-market.html.

[10] "12 Billion Pound NHS Computer System is Scrapped. . . and It's All YOUR Money That Labor Poured Down the Drain," Daily Mail, Sept. 22, 2011, http://www.dailymail.co.uk/news/article-2040259/NHS-IT-project-failure-Labours-12bn-scheme-scrapped.html; "NHS Research System Could Breach Patient Confidentiality," Computer Weekly, Feb. 8, 2011, http://www.computerweekly.com/news/1280095089/NHS-research-system-could-breach-patient-confidentiality?vgnextfmt=print; "For Sale: Your Most Intimate Secrets. . . Thanks to the National NHS Database," Daily Mail, April 22, 2010, http://www.dailymail.co.uk/news/article-1267892/Putting-health-records-national-NHS-database-save-lives-deeply-disturbing-questions-remain.html?printingPage=true; "Patients Win Right to Keep Records Off NHS Computer," The Guardian, Dec. 15, 2006, http://www.guardian.co.uk/society/2006/dec/16/health.epublic/print.

[11] See NASA v. Nelson, Whalen v. Roe, 429 U.S. 589, 599-600 (1977); Nixon v. Administrator of General Services, 433 U.S. 425, 457 (1977).

[12] Griswold v. Connecticut, 381 U.S. 479 (1965).

[13] Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

[14] Fraternal Order of Police v. City of Philadelphia, 812 F.2d 105, 112-113 (3rd Cir. 1987).

[15] The Privacy Act of 1974, Pub. L. 93-579, Section 2(a)(4), 88 Stat. 1896.

[16] 65 Fed. Reg. at 82,468 (Dec. 28, 2000).

[17] 65 Fed. Reg. at 82,464.

[18] Department of Health and Human Services findings, 65 Fed. Reg. 82,467/2 (Dec. 28, 2000).

[19] 45 C.F.R. § 164.104; HITECH Act, section 13404(a).

[20] 45 C.F.R. § 164.520(b)(1)(iv).

[21] The Glossary of this report includes a widely accepted definition of "health information privacy" which has been adopted by the National Committee on Vital and Health Statistics – the organization on which the Secretary of HHS is to rely in implementing HIPAA. See section 1172(f) of HIPAA.

[22] See HHS finding, 65 Fed. Reg. at 82,472/3; American Medical Association, Principles of Ethics, section IV; American Psychoanalytic Association, General Principles of Ethics, section IV; 45 C.F.R. § 164.502(a); 67 Fed. Reg. at 53,2123.

[23] Freudenheim, Milt. "Breaches Lead to Push to Protect Medical Data." The New York Times, May 30, 2011. Web. http://www.nytimes.com//2011/05/31/business/31privacy.html.

[24] Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach.

[25] Thompson, Don. "Theft of Data on 4M Patients Part of Wider Problem." Yahoo! Finance, Associated Press, Nov. 17, 2011. Web. http://finance.yahoo.com/news/theft-data-4m-patients-part-232412872.html.

[26] Goedert, Joseph. "TRICARE, the U.S. Military Health Program, Has Reported a Massive Breach Affecting Protected Health Information for 4.9 Million Patients." Health Data Management, Source Media, Sept. 29, 2011. Web. http://www.healthdatamanagement.com/news/breach-tricare-notification-hipaa-privacy-43288-1.html?zkPrintable=true.

[27] Thompson, Don. "Theft of Data on 4M Patients Part of Wider Problem." Yahoo! Finance, Associated Press, Nov. 17, 2011. Web. http://finance.yahoo.com/news/theft-data-4m-patients-part-232412872.html.

[28] Sack, Kevin. "Patient Data Posted Online in Major Breach of Privacy." The New York Times, Sept. 8, 2011. Web. http://www.nytimes.com//2011/09/09/us/09breach.html.

[29] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[30] Wolf, Isaac, "Docs Withhold Records from Victims of Medical ID Theft," Scripps News, Mar. 16, 2011. Web. http://scrippsnews.com/content/docs-withhold-records-victims-medical-id-theft; Wilson, Michael and William K. Rashbaum, "Real Patients, Real Doctors, Fake Everything Else," The New York Times, Oct. 13, 2010. Web. http://www.nytimes.com//2010/10/14/nyregion/14fraud.html.

[31] Barrett, Larry. "Data Breaches Continue to Plague Health Care Orgs." eSecurity Planet, Aug. 3, 2010. Web. http://www.esecurityplanet.com/trends/article.php/3896676/Data-Breaches-Continue-to-Plague-Health-Care-Orgs.htm. Identity Theft Resource Center 2010 Report issued 12/29/10. http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20101229.pdf.

[32] Greenwald, Judy. "Breach concerns rise for health care firms." BusinessInsurance.com, Nov. 27, 2011. Web. http://www.businessinsurance.com/article/20111127/NEWS07/311279968?elq_mid=16777&elq_cid=1094517.

[33] McKay, Jim. "Identity Theft Steals Millions from Government Health Programs." GovTech.com, Feb. 12, 2008. Web. 6 Sept. 2011 . http://www.govtech.com/security/Identity-Theft-Steals-Millions-from-Government.html.

[34] PricewaterhouseCoopers Health Research Institute, "Old Data Learns New Tricks: Managing Patient Privacy and Security on a New Data-sharing Playground," PricewaterhouseCoopers, Sept. 2011; "Health industry under-prepared to protect patient privacy; risk of data breaches rise with new access to digital health information, says PwC," Sept. 22, 2011, Web, http://www.pwc.com/us/en/press-releases/2011/health-industry-under-prepared.jhtml; Terry, Ken, "Healthcare industry poorly protecting patient privacy," Fierce Health IT, Sept. 22, 2011, Web, http://www.fiercehealthit.com/story/healthcare-industry-not-protecting-patient-privacy-well/2011-09-22.

[35] "Medicare Fraud: A $60 Billion Crime." 60 Minutes, CBS News, Sept. 5, 2010. Web. http://www.cbsnews.com/stories/2009/10/23/60minutes/main5414390.shtml.

[36] MiddleGate Med proprietary research, May 2011.

[37] McKay, Jim. "Identity Theft Steals Millions from Government Health Programs." GovTech.com, Feb. 12, 2008. Web. Sept. 6, 2011. http://www.govtech.com/security/Identity-Theft-Steals-Millions-from-Government.html.

[38] McKay, Jim. "Identity Theft Steals Millions from Government Health Programs." GovTech.com, Feb. 12, 2008. Web. Sept. 6, 2011. http://www.govtech.com/security/Identity-Theft-Steals-Millions-from-Government.html.

[39] Sack, Kevin. " Patient Data Landed Online After a Series of Missteps." The New York Times, Oct. 5, 2011. Web. http://www.nytimes.com/2011/10/06/us/stanford-hospital-patient-data-breach-is-detailed.html.

[40] Cyber-Ark. "Cyber-Ark Global Survey Shows External Cyber-Security Risks Will Surpass Insider Threats." Cyber-Ark, Apr. 14, 2011. Web. http://www.cyber-ark.com/news-events/pr_20110413.asp.

[41] Veriphyr. "2011 Survey of Patient Privacy Breaches." Rep. Veriphyr, Aug. 2011. Web. http://blog.veriphyr.com/2011/08/over-70-of-healthcare-providers.html.

[42] Ornstein, Charles. "Fawcett's cancer file breached." Los Angeles Times, Apr. 3, 2008. Web. http://articles.latimes.com/2008/apr/03/local/me-farrah3.

[43] Ornstein, Charles. "Farrah Fawcett: 'Under a microscope' and holding onto hope." Los Angeles Times, May 11, 2009. Web. http://www.latimes.com/entertainment/news/la-et-fawcett-interview11-2009may11,0,5790379.story.

[44] Innes, Stephanie. "3 UMC workers fired for invading records." Arizona Daily Star, Jan. 13, 2011. Web. http://azstarnet.com/news/local/article_a2645584-906d-50a9-84a4-645d4d4a94b9.html.

[45] Harris Interactive. "Millions Believe Personal Medical Information Has Been Lost or Stolen: Issue a roadblock to acceptance of electronic health record systems." Healthcare News 8.7, July 30, 2008. Web. http://www.harrisinteractive.com/vault/HI_HealthCareNews2008Vol8_Iss07.pdf.

[46] Westin, Dr. Alan, and Harris Interactive. "How the Public Views Privacy and Health Research." Nov. 2007. Web. http://www.ftc.gov/os/comments/healthcarewrkshp/534908-00001.pdf.

[47] The National Committee on Vital and Health Statistics. "Privacy and Confidentiality in the Nationwide Health Information Network." June 22, 2006. Web. http://ncvhs.hhs.gov/060622lt.htm.

[48] 65 Fed. Reg. at 82,464-465.

[49] Patient Privacy Rights and Zogby International. "2000 Adults' Views on Privacy, Access to Health Information and Health Information Technology." Aug. 2010. Web. http://patientprivacyrights.org/wp-content/uploads/2010/11/Zogby-Result-Illustrations.pdf.

[50] 65 Fed. Reg. at 82,760/2 and 82,767.

[51] 65 Fed. Reg. at 82,767.

[52] 65 Fed. Reg. at 82,779.

[53] 65 Fed. Reg. at 82,778.

[54] "National Strategy for Trusted Identities," supra, at p. 2.

[55] Id. at p. 11.

[56] Id. at p. 4.

[57] "Accelerating Electronic Health Records Adoption and Meaningful Use." HHS News Release, August 5, 2010. Web. http://www.hhs.gov/news/press/2010pres/08/20100805c.html; HITECH Act, section 3001(c)(3).

[58] Verizon and Secret Service. "2010 Data Breach Investigations Report," July 2010, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf; Messmer, Ellen, "Biggest insider threat? Sys admin gone rogue," Network World, Sept. 27, 2010, http://www.networkworld.com/news/2010/092710-insider-threats.html?ap1=rcb.

[59] Brook, Christopher. "Anonymous Hacks, Leaks E-Mails, Voicemails of California Special Agent." Nov. 21, 2011. Web. http://threatpost.com/en_us/blogs/anonymous-hacks-leaks-e-mails-voicemails-doj-agent-112111.

[60] Terry, Ken. "Healthcare industry poorly protecting patient privacy." Fierce Health IT, Sept. 22, 2011. Web. http://www.fiercehealthit.com/story/healthcare-industry-not-protecting-patient-privacy-well/2011-09-22.

[61] Thompson, Don and Marcus Wohlsen. "Theft of data on 4M patients part of a wider problem." Boston Globe, Nov. 17, 2011. Web. http://www.boston.com/business/technology/articles/2011/11/17/theft_of_data_on_4m_patients_part_of_wider_problem/.

[62] Roy Adar. "Perceived Security vs. Real Vulnerability: Is Your Data at Risk?" TechnNewsWorld, Mar. 10, 2010. http://www.technewsworld.com/story/69506.html.

[63] Arena, Jill, Chad Boeckmann, Rebecca Herold, Rick Kam, and Robert Siciliano. "Mobile Devices Pose New Security Risks for Patients; Five Experts Share Insights on MHealth." Interview. Idexperts: Complete Data Breach Care. Idexperts, July 20, 2011. Web. http://www2.idexpertscorp.com/press/healthcare-news/mobile-devices-pose-new-security-risks/.

[64] Ibid.

[65] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[66] PricewaterhouseCoopers. "Health industry under-prepared to protect patient privacy; risk of data breaches rise with new access to digital health information, says PwC." Sept. 22, 2011. Web. http://www.pwc.com/us/en/press-releases/2011/health-industry-under-prepared.jhtml.

[67] Breach Notification Rule Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html. Title 45 Part 164.504 (e) Security and Privacy Uses and disclosures: Organizational requirements Business Associates contracts.

[68] Anderson, Howard. "Updating the Breach Scorecard." Healthcare Info Security, Oct. 24, 2011. Web. http://www.healthcareinfosecurity.com/articles.php?art_id=4175.

[69] PricewaterhouseCoopers. "Health industry under-prepared to protect patient privacy; risk of data breaches rise with new access to digital health information, says PwC." Sept. 22, 2011. Web. http://www.pwc.com/us/en/press-releases/2011/health-industry-under-prepared.jhtml.

[70] Shaw, Thomas. "Information and Security, A Practical Guide for Global Executives, Lawyers and Technologists." American Bar Association, Feb. 17, 2011. pp. 279-83.

[71] http://www.nist.gov/itl/csd/cloud-012412.cfm.

[72] Gartner Group. "Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010." Gartner Group, June 22, 2010. Web. http://www.gartner.com/it/page.jsp?id=1389313.

[73] Mika, Karin and Barbara J. Tyler. "Cybermedicine, Telemedicine, and Data Protection in the United States." Health Information Systems: Concepts, Methodologies, Tools, and Applications. IGI Global, 2010. pp. 274-296. Web. http://www.igi-global.com/chapter/cybermedicine-telemedicine-data-protection-united/49869.

[74] United States. Department of Defense. "Department of Defense Strategy for Operating in Cyberspace." Defense.gov. Department of Defense, July 2011. Web. http://www.defense.gov/news/d20110714cyber.pdf.

[75] "Cybersecurity Today: Trends, Risk Mitigation & Research." The Austin Forum on Science, Technology & Society, Sept 2011. Web. http://www.austinforum.org/presentations/cybersecurity.pdf.

[76] Satter, Raphael G. "Britain Warns against State-sponsored Cyberattacks." MSNBC, Jan. 5, 2012. Web. http://www.msnbc.msn.com/id/45137676/ns/technology_and_science-security/t/britain-warns-against-state-sponsored-cyberattacks/.

[77] Anderson, Howard. "Permanent HIPAA Audit Program Coming." Health Care InfoSecurity, Nov. 17, 2011. Web. http://www.healthcareinfosecurity.com/articles.php?art_id=4253&rf=2011-11-18-eh&elq=89640e541db34f78a2b22b4b17aa13e0&elqCampaignId=839.

[78] http://webstore.ansi.org/packages/it_security.aspx.

[79] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[80] http://webstore.ansi.org/packages/it_security.aspx.

[81] HITRUST. "Common Security Framework." Web. http://www.hitrustalliance.net/commonsecurityframework/.

[82] Health Information Technology. Kaiser EDU. Web. http://www.kaiseredu.org/Issue-Modules/Health-Information-Technology/Background-Brief.aspx.

[83] Reducing Paperwork and Administrative Costs. "Provisions of the Affordable Care Act." 2012. Web. http://www.healthcare.gov/law/timeline/full.html.

[84] PricewaterhouseCoopers. "Health industry under-prepared to protect patient privacy; risk of data breaches rise with new access to digital health information, says PwC." Sept. 22, 2011. Web. http://www.pwc.com/us/en/press-releases/2011/health-industry-under-prepared.jhtml.

[85] Ibid.

[86] HIMSS Security Survey, supported by MGMA. Nov. 2011. Web. http://www.himss.org/content/files/2011_HIMSS_SecuritySurvey.pdf.

[87] Society of Corporate Compliance and Ethics and Health Care Compliance Association. "Stress, Compliance and Ethics." Jan. 2012 Web. http://www.hcca-info.org/staticcontent/StressSurvey_report.pdf.

[88] American National Standards Institute (ANSI), The Santa Fe Group / Shared Assessments Program, Internet Security Alliance (ISA), PHI Project Survey.

[89] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[90] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[91] William B. Baker, Kathleen A. Kirby & Amy E. Worlton. "Beware of Costly Data Breaches." Mass Media Headlines, Sept. 2011. Web. http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=5&id=7505&&elq_mid=16002&elq_cid=1094517#page=1.

[92] Jones, Stephanie. "Protecting Government Information." American City and County, Aug. 1, 2011. Web. http://americancityandcounty.com/security/government-information-protection-201108/index.html.

[93] 45 CFR 164, Subpart A.

[94] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[95] Fisher, Luchina. "Musician Makes Music Out of Feud with United Airlines." ABC News, July 9, 2009. Web. Sept. 6, 2011 http://abcnews.go.com/Entertainment/Business/story?id=8043639&page=1.

[96] Serwin, Andy. "Study on Privacy Demographics." The Lares Institute Blog. The Lares Institute, Sept. 9, 2011. Web. Jan. 4, 2012. http://www.laresinstitute.com/blog/study-on-privacy-demographics.

[97] Forrester Research, "Calculating the Cost of a Security Breach," cited in Sharon Gaudin, "Security Breaches Cost $90 To $305 Per Lost Record," InformationWeek, April 11, 2007. Web. http://www.informationweek.com/news/199000222.

[98] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[99] Brewin, Bob. "Groups urge TRICARE to provide credit monitoring for victims of records theft." NextGov, Oct. 3, 2011. Web. http://www.nextgov.com/nextgov/ng_20111003_9355.php.

[100] Breach Notification Rule, Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act. 2011. Web. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.

[101] Edwards, Cliff and Yasu, Mariko. "Sony Offers Network Users Free Identity-Theft Service after Hacker Attack." Bloomberg, May 6, 2011. Web. http://www.bloomberg.com/news/2011-05-06/sony-offers-network-users-free-identity-theft-service-after-hacker-attack.html.

[102] Greenwald, Judy. "Breach concerns rise for health care firms." Business Insurance, Nov. 27, 2011. Web. http://www.businessinsurance.com/article/20111127/NEWS07/311279968?elq_mid=16777&elq_cid=1094517.

[103] Dell SecureWorks. "Security 101: Cost of a Breach" Oct 2007. Web. http://www.secureworks.com/research/newsletter/2007-10/.

[104] U.S. Department of Health and Human Services. "UCLA Health System Settles Potential HIPAA Privacy and Security Violations." U.S. Department of Health and Human Services July 6, 2011. Web. Sept. 6, 2011. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/UCLAHSracap.pdf.

[105] Ibid.

[106] Jones, Stephanie. "Cyber Security Risks a Matter of When, Not If." Insurance Journal, Sept. 19,2011. Web. http://www.insurancejournal.com/magazines/ideaexchange/2011/09/19/215936.htm?elq_mid=16002&elq_cid=1094517.

[107] Vijayan, Jaikumar. "Stanford Hospital blames contractor for data breach." Computer World, Oct. 6, 2011. Web. http://www.computerworld.com/s/article/9220626/Stanford_Hospital_blames_contractor_for_data_breach?source=CTWNLE_nlt_dailyam_2011-10-07&elq_mid=16002&elq_cid=1094517.

[108] Goedert, Joseph. "TRICARE Hit with $4.9 Billion Suit Following Breach." HDMBreaking News, Oct. 17, 2011. Web. http://www.healthdatamanagement.com/news/breach-tricare-notification-hipaa-privacy-43404-1.html.

[109] Morris, Duane. "The Ever Expanding Data Breach Notification Laws… Texas Amendment Requires Notification to Affected Residents in All 50 States." Oct. 6, 2011. Web. http://blogs.duanemorris.com/duanemorristechlawblog/entry/the_ever_expanding_data_breach.

[110] "State Agency Fines Health Net for Data Breach" Health Data Management, Nov. 9, 2011. Web. http://www.healthdatamanagement.com/news/security-breach-health-net-connecticut-insurance-department-fine-41319-1.html.

[111] HIPAA, section 1177.

[112] HITECH Act, section 13410(d).

[113] HITECH Act, section 13410(c)(2); 45 C.F.R. § 160.401.

[114] HITECH Act, section 13410(e).

[115] "State Privacy Breach Laws My Trump HIPAA/HITECH." E is for ERISA, July 11, 2011. Web. http://eforerisa.wordpress.com/2011/07/11/state-privacy-breach-laws-may-trump-hipaahitech/.

[116] HITECH Act, section 13410(c).

[117] Ibid.

[118] PricewaterhouseCoopers. "Health industry under-prepared to protect patient privacy; risk of data breaches rise with new access to digital health information, says PwC." Sept. 22, 2011. Web. http://www.pwc.com/us/en/press-releases/2011/health-industry-under-prepared.jhtml.

[119] Ponemon. "Ponemon Institute's Second Annual Survey 2011." Web. http://www.experian.com/data-breach/newsletters/ponemon-institute.html

[120] According to Dr. Sean Scorvo, MD, ER physician, and CEO of MiddleGate Med, from studies conducted by MiddleGate Med, an emergency room fraud alert service.

[121] Ponemon Institute LLC. "Second Annual Benchmark Study on Patient Privacy & Data Security." Sponsored by ID Experts, Dec. 2011. Web. http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf.

[122] Ko, Myung. "Impact Of Security Breaches On Firm Performance." Journal of Information Technology Management, 2006th ser. XVII, 2 (2006), Jan. 5, 2012.

Project Leadership

The **American National Standards Institute** (ANSI – www.ansi.org) is a private non-profit organization whose mission is to enhance U.S. global competitiveness and the American quality of life by promoting, facilitating, and safeguarding the integrity of the voluntary standards and conformity assessment system. The ANSI Identity Theft Prevention and Identity Management Standards Panel (IDSP) is a cross-sector coordinating body that facilitates the timely development, promulgation, and use of voluntary consensus standards and guidelines that will equip and assist the private sector, government, and consumers in minimizing the scope and scale of identity theft and fraud.

The **Shared Assessments Program** (www.sharedassessments.org) was created by leading financial institutions, the Big Four accounting firms, and key service providers to inject standardization, consistency, speed, efficiency, and cost savings into the service provider assessment process. The Shared Assessments Program is the premiere provider of vendor risk management solutions and tools, which focus on establishing industry best practices, lowering the cost and improving the efficiency of the vendor risk assessment process. Through membership and use of the Shared Assessments tools, Shared Assessments offers outsourcers and their service providers a faster, more efficient, and less costly means of conducting rigorous assessments of controls for security, privacy, and business continuity. Since its inception, the Shared Assessments Program has been managed by The Santa Fe Group, a strategic consulting company.

The **Internet Security Alliance** (ISA – www.isalliance.org) is a multi-sector trade association established in collaboration with Carnegie Mellon University in 2000. ISA represents an array of organizations concerned with information security from the aviation, banking, communications, defense, education, financial services, insurance, manufacturing, security, and technology sectors. The ISA mission is to combine advanced technology with business economics and public policy to create a sustainable system of world-wide cybersecurity. ISA advocates a modernized social contract between industry and government that would create market-based incentives to motivate enhanced security of cyber systems. ISA provides its members with technical, business, and public policy services to assist them in fulfilling their mission.

Premium Sponsors

Clearwater Compliance (www.clearwatercompliance.com) helps covered entities, business associates, and their subcontractors assess their HIPAA-HITECH compliance programs, identify gaps, and prioritize remediation efforts to ensure the greatest return on capital and resource investments. With the help of proprietary, easy-to-use software, templates, and toolkits, compliance officers can quickly establish a practical corrective action plan tailored specifically to their organization and create a strong competitive positioning as it relates to safeguarding PHI.

DriveSavers Data Recovery (www.drivesaversdatarecovery.com), the worldwide leader in data recovery services, provides fast, reliable, and certified secure data recovery service. DriveSavers is the only company in the data recovery industry to post proof of annual, company-wide SAS 70 Type II Audit Reports and its compliance with the HIPAA security rule. DriveSavers adheres to U.S. government security protocols, the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act of 2002, the Family Educational Rights and Privacy Act, and the National Institute of Standards and Technology's SP 800.34 (Rev.1). DriveSavers engineers are certified in all leading encryption and forensics technologies and operate a Certified ISO 5 cleanroom.

Partner Sponsors

American National Standards Institute
25 West 43rd Street, Fourth Floor
New York, NY 10036
T: 212.642.4900
E: info@ansi.org
www.ansi.org

Shared Assessments
3 Chamisa Drive, North Suite 2
Santa Fe, NM 87508
T: 505.466.6434
E: sharedassessments@santa-fe-group.com
www.sharedassessments.org

Internet Security Alliance
2500 Wilson Boulevard
Arlington, VA 22201
T: 703.907.7799
E: info@isalliance.org
www.isalliance.org

"Patients historically trust their doctors to be data stewards of their private health information in paper charts. As healthcare moves from paper to digital in the new age of networked electronic health records, this important publication is convincing and educational about how the broader healthcare system must work hard to earn the same trust that patients have in their doctors to protect their personal and private health information."

– Dr. Robert Wah, Chief Medical Officer, CSC; Chairman-elect, American Medical Association Board of Trustees

"The PHI study is the front end of a much needed effort to get ahead of those who would penetrate the data systems of our health care providers."

– John R. Powers, Commissioner and Executive Director, President's Commission on Critical Infrastructure Protection, 1996-98; Career Senior Executive and FEMA Regional Director, 1993-95

"An indispensable resource for those wrestling with the challenges of PHI security risk."

– Dr. Michael Kraten, Assistant Professor of Accounting, Providence College; President, Enterprise Management Corporation

"This publication is a must read. It provides not only very useful background information, but also numerous examples of what can happen when appropriate steps are not taken to ensure protected health information integrity. Beyond that, it offers a framework for organizations to assess their security and compliance programs, and it provides a tool for estimating the impact of security breaches on multiple levels.

"No one – not C-level executives, not health care administrators, not Boards of Directors – can afford to ignore its message."

– Dr. John Fox, President, FFC Computer Services, Inc.

"In this era of emerging awareness of the responsibility and legal requirement to ensure the confidentiality, integrity, and availability of individuals' protected health information (PHI), as well as the consequences of disregard, business leaders and executives are quickly coming to realize several maxims: first, it's about business risk management rather than an 'IT problem;' second, it requires a programmatic approach; and, third, the C-suite owns this one.

"Smart leaders and managers who care about revenue and asset and reputation preservation will benefit greatly from the research and valuable recommendations found in this insightful paper."

– Bob Chaput, CEO and Founder, Clearwater Compliance LLC

"Every organization in the health care ecosystem needs to implement safeguards and controls to protect PHI and minimize financial, reputational, and legal ramifications. This report provides an invaluable five-step method for strengthening privacy and security programs that will help significantly reduce the probability of a breach.

"CISOs, CIOs, and IT security at every health care organization should have this publication in their hands today!"

– Michael Hall, CISO, DriveSavers Data Recovery, Inc.

"Health care is one of the most-breached industries. Health care providers and supporting organizations don't currently have sufficient security and privacy budgets, including adequate processes and resources, to protect sensitive patient data. This report will help them understand what they need to do to augment their efforts."

– Dr. Larry Ponemon, Chairman and Founder, Ponemon Institute

The Financial Impact of Breached Protected Health Information

APPENDIX A

Glossary of Terms and Acronyms

To accurately understand the legal obligations associated with safeguarding protected health information (PHI), it is important to have an understanding of key terms. The following definitions are a summary of key terms and acronyms used in *The Financial Impact of Breached Protected Health Information* report and its appendices. These are based on definitions found in common authoritative texts and in case law. They do not necessarily constitute a definition that may be universally applied in any situation. Should the reader have a question as to whether a particular definition fits a particular scenario, the advice of appropriate legal counsel should be sought.

Access

HIPAA Administrative Simplification Regulation Text 45 CFR § 164.304

The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Ability to make use of any information system (IS) resource. – *SOURCE: SP 800-32*

Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. – *SOURCE: CNSSI-4009*

Administrative Safeguards

HIPAA Administrative Simplification Regulation Text 45 CFR §164.304

Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Ability to make use of any information system (IS) resource. – *SOURCE: SP 800-32*

Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. – *SOURCE: SP 800-66*

Attack

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. – *SOURCE: SP 800-32*

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. – *SOURCE: CNSSI-4009*

Audit

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. – *SOURCE: SP 800-32*

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. – *SOURCE: CNSSI-4009*

Availability

HIPAA Administrative Simplification Regulation Text 45 CFR §164.304

The property that data or information is accessible and useable upon demand by an authorized person.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Ensuring timely and reliable access to and use of information. – *SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542*

The property of being accessible and useable upon demand by an authorized entity. – *SOURCE: CNSSI-4009*

Breach

42 USC 17921(1)

(A) In general: The term "breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
(B) Exceptions: The term "breach" does not include — (i) any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if — (I) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and (II) such information is not further acquired, accessed, used, or disclosed by any person; or (ii) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and (iii) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

HIPAA Administrative Simplification Regulation Text Section 45 CFR §164.402

The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information. (2) Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate

HIPAA Administrative Simplification Regulation Text 45 CFR §160.103

(1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate of another covered entity.

Cloud Computing

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

NIST Special Publication 800-146

A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (cloud software as a service [SaaS], cloud platform as a service [PaaS], and cloud infrastructure as a service [IaaS]); and four models for enterprise access (private cloud, community cloud, public cloud, and hybrid cloud).

Note: Both the user's data and essential security services may reside in and be managed within the network cloud. – *SOURCE: CNSSI-4009*

Confidentiality

HIPAA Administrative Simplification Regulation Text 45 CFR § 164.304

The property that data or information is not made available or disclosed to unauthorized persons or processes.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. – *SOURCE: SP 800-53; SP 800-53A; SP 800-18; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542*

National Committee on Vital and Health Statistics, Recommendations on Privacy and Confidentiality, 2006-2008

The obligations of those who receive information to respect the privacy interests of those to whom the data relate.

Covered Entities

HIPAA Administrative Simplification Regulation Text 45 CFR § 164.103

(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Cyber Attack

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. – *SOURCE: CNSSI-4009*

Data

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

A subset of information in an electronic format that allows it to be retrieved or transmitted. – *SOURCE: CNSSI-4009*

Electronic Health Records (EHR)

42 USC 17921(5)

The term "electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

42 USC §3000(13)

The term "qualified electronic health record" means an electronic record of health-related information on an individual that – (A) includes patient demographic and clinical health information, such as medical history and problem lists; and (B) has the capacity – (i) to provide clinical decision support; (ii) to support physician order entry; (iii) to capture and query information relevant to health care quality; and (iv) to exchange electronic health information with, and integrate such information from, other sources.

Encryption

HIPAA Administrative Simplification Regulation Text 45 CFR §164.304

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. – *SOURCE: FIPS 185*

The process of changing plaintext into ciphertext for the purpose of security or privacy. – *SOURCE: SP 800-21; CNSSI-4009*

HHS

The U.S. Department of Health and Human Services

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191

HITECH

The Health Information Technology for Economic and Clinical Health Act, Public Law 111-5

Identity Theft

18 U.S.C. §1028

(a) Whoever, in a circumstance described in subsection (c) of this section — (1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document; (2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority; (3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents; (4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States; (5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used; (6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority; (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid, or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law; or (8) knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification.

18 U.S.C. §1028

(a) The term "identity theft" means a fraud committed or attempted using the identifying information of another person without authority. (b) The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any — (1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) Unique electronic identification number, address, or routing code; or (4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029[e]).

Pub. L. 108–159, sec 111; 15 U.S.C. 1681a

The term 'identity theft' means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.

Incident

HIPAA Administrative Simplification Regulation Text 45 CFR § 164.304

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices – *SOURCE: SP 800-61*

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. – *SOURCE: FIPS 200; SP 800-53*

An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. – *SOURCE: CNSSI-4009*

Individually Identifiable Health Information

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191

HIPAA Administrative Simplification Regulation Text 45 CFR §160.103

Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Integrity

HIPAA Administrative Simplification Regulation Text 4534 CFR §164.304

The property that data or information have not been altered or destroyed in an unauthorized manner.

Malware

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. – *SOURCE: SP 800-83*

Media

HIPAA Administrative Simplification Regulation Text 45 CFR §160.103

Electronic media means: (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, large scale integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. – *SOURCE: FIPS 200; SP 800-53; CNSSI-4009*

Medical Identity Theft

The World Privacy Forum, Medical Identity Theft: The Information Crime that Can Kill You, Spring 2006

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as insurance information – without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.

Mobile Devices

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory).

Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). – *SOURCE: SP 800-53*

NIST

National Institute of Standards and Technology

Personally Identifiable Information (PII)

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including: (i) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Physical Safeguards

HIPAA Administrative Simplification Regulation Text 45 CFR §164.304

Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy

National Committee on Vital and Health Statistics, Recommendations on Privacy and Confidentiality, 2006-2008

Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.

Proprietary Information

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the government or to the public without restriction from another source. – *SOURCE: CNSSI-4009*

Protected Health Information (PHI)

HIPAA Administrative Simplification Regulation Text 45 CFR §160.103

Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.

Risk

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. – *SOURCE: FIPS 200*

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. – *SOURCE: SP 800-60*

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Note: Information system–related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. – *SOURCE: SP 800-53*

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. – *SOURCE: CNSSI-4009*

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. Adverse impacts to the nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security. – *SOURCE: SP 800-37; SP 800-53A*

The probability that one or more adverse events will occur. – *SOURCE: SP 800-61*

Security

National Committee on Vital and Health Statistics, Recommendations on Privacy and Confidentiality, 2006–2008

Physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. – *SOURCE: CNSSI-4009*

Technical Safeguards

HIPAA Administrative Simplification Regulation Text 45 CFR §160.103

The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Threat

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. – *SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009*

The potential source of an adverse event. – *SOURCE: SP 800-61*

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. – *SOURCE: FIPS 200*

Unauthorized Disclosure

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

An event involving the exposure of information to entities not authorized access to the information. – *SOURCE: SP 800-57; CNSSI-4009*

The Financial Impact of Breached Protected Health Information

APPENDIX B

Legal and Regulatory Liabilities

Note: These research notes have been substantially edited down so as to supplement but not duplicate information included in the PHI project report.

The Impact of Electronic Health Information on Health Information Privacy: The Growth in Reported Privacy Violations

According to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), nearly 20 million Americans have had the privacy of their electronic protected health information (PHI) breached in nearly 400 incidents involving more than 500 individuals between September 2009 and February 2012.[1] The most common cause of these breaches was theft.

The privacy of thousands of additional individuals has been breached in incidents involving less than 500 individuals. From April 2003 through July 2011, OCR received more than 62,000 complaints of violations of *The Health Insurance Portability and Accountability Act of 1996* (HIPAA) Privacy Rule. Another 420 complaints were received by OCR from October 2009 through July 2011, alleging violations of the HIPAA Security Rule. OCR has referred more than 499 cases to the Department of Justice for possible criminal prosecution. Of course, OCR has no authority to track or investigate privacy violations by entities other than covered entities and their business associates.

1. The Costs of Electronic Privacy Breaches

Four major types of "enterprise" costs resulting from inadequate protection of electronic health information are: (a) criminal and civil penalties for failing to comply with health information privacy laws; (b) damages for breach of privacy and negligence; (c) legal and consulting fees in connection with enforcement actions and private law suits; and (d) loss of business and reputation.[2] While not direct "enterprise" costs, higher costs are also incurred by the health care system when individuals fail to obtain needed health care due to privacy concerns.[3] It has been estimated that the direct cost of health care data breaches is $371 per record and that data breaches cost the health care industry approximately $6.5 billion a year.[4]

Penalties for violations of privacy laws are the easiest to quantify. OCR recently invoked the HIPAA Privacy Rule and imposed a civil monetary penalty of $4.3 million on a health plan that failed to provide 41 patients with access to their health information and then failed to respond to OCR's complaint and subsequent investigative demands.[5] OCR also recently agreed to a settlement of $1 million with a physician group practice specializing in infectious diseases due to the loss of records of

192 patients, including patients with HIV/AIDS, when an employee left the records on a subway train.[6] More recently, OCR agreed to accept a payment of $865,500 from a university health care provider for allegedly failing to prevent an employee from improperly viewing electronic health records (EHRs) of celebrity patients and failing to sanction the employee.[7] A psychotherapist was recently indicted on federal criminal charges stemming from a HIPAA Privacy Rule violation for allegedly disclosing a patient's mental health treatment information to an "agent" of the patient's employer without the patient's authorization and on the false pretense that the patient was an imminent threat to the public while knowing otherwise.[8]

OCR has provided training to state attorneys general in how to institute legal proceedings for health information privacy violations.[9] A major health plan recently agreed to pay a $100,000 fine levied by a state attorney general involving an electronic health privacy breach.[10] Another state attorney general agreed to a $250,000 settlement of a HIPAA violation in which a health insurer lost a computer disk containing the names, addresses, and health and financial information of more than 2 million customers.[11]

OCR recently hired an accounting firm to perform 150 HIPAA privacy and security compliance audits by the end of 2012.[12] Given that the Office of the Inspector General of HHS published a report that seven hospitals randomly reviewed for compliance with health information privacy and security compliance had 151 "vulnerabilities" in systems and controls – 124 of which were categorized as "high impact"[13] – it is likely that audits will find deficiencies in compliance.

In addition to federal and state fines and penalties, private lawsuits for breach of health information privacy can also result in large awards or settlements. For example, the U.S. Department of Veterans Affairs (VA) agreed to pay a $20 million settlement for the theft of a laptop computer from an employee's home, containing information on 26.5 million VA patients, even though the items were later turned in and there was no evidence that the databases had been accessed.[14] A national company with eye examination and eyewear subsidiaries settled a class action lawsuit brought by 1.4 million consumers for $20 million, following allegations that the eye examiners improperly disclosed health histories to the eyewear retailer for the purposes of marketing eyewear.[15] Recently, the health care program for the U.S. Department of Defense was sued for $4.9 billion after backup tapes containing health and other personal information on 4.9 million military personnel were stolen from the automobile of a contractor for the program.[16]

The *Health Information Technology for Economic and Clinical Health* (HITECH) *Act* enacted in February 2009, which expanded privacy protections of the HIPAA Privacy Rule, has been projected to increase health care spending under the Medicare and Medicaid programs by $32.7 billion from 2009 through 2019.[17] That cost was projected to be decreased to $20.8 million if 45% of hospitals and 65% of physicians adopt EHR systems by 2019. As of 2009, only about 1.5% of U.S. hospitals had comprehensive EHR systems (i.e., present in all clinical units), 7.6% had a basic system, while only about 5% of physicians had a fully functional EHR system that is interoperable.[18] The rising cost of electronic privacy breaches does not appear to have been factored into the cost of implementing EHR systems nationwide. Investment in protection of the privacy of health care is critical to the adoption of EHRs to preserve the public's confidence that private health information will be adequately protected, and is essential in avoiding further escalation of health care costs.

2. The Public's Perception of Health Information Privacy

What is the public's expectation of health information privacy? After one of the largest rulemakings in the history of the agency, HHS determined when it issued the original HIPAA Privacy Rule that

> ". . . the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers."[19]

According to HHS, this essential transaction cannot occur without a relationship of trust.[20] For that trust to exist, individuals must believe that the privacy of their health information will be protected by those who handle it.[21] Trust must also exist for the public to accept the use of electronic health information systems to store and transmit their personal health information.[22]

Legal Liability Arising from Electronic Health Information Systems: Sources of Health Information Privacy Liability

Management and reduction of the financial and business liability arising from mishandling personal health information is only possible with a clear understanding of the privacy rights of patients and customers and the requirements and enforcement mechanisms of health information privacy laws and professional ethics. In other words, enterprises that handle electronic health information must be aware of their customer privacy expectations which form the basis of laws, regulations, and what is considered reasonable in the context of tort liability.

1. The Constitutional Right to Privacy

Even though the Constitution only protects individuals from privacy intrusions by governments rather than by private entities,[23] individuals employed by governmental entities (e.g., governmentally operated hospitals) can be sued in their personal capacities for violating privacy rights they should have known existed.[24] For example, a swimming coach employed by a county high school was successfully sued in his individual capacity under the *Civil Rights Act* for violating the constitutionally protected privacy rights of a young woman on the team when he disclosed the results of a pregnancy test he required her to take.[25] A police officer was successfully sued for the wrongful death of a young man who committed suicide after the officer threatened to disclose his sexual orientation to his family.[26]

Most recently, in 2012, the Supreme Court unanimously held that Americans have a right to privacy with respect to the government for information collected using electronic technology, and that this protection is afforded by the Fourth Amendment right to be free from "unreasonable searches and seizures." The basis of the right to privacy can be either the intent of the framers of the Constitution at the time it was drafted or an individual's "reasonable expectation" of privacy today. As one justice said in a concurring opinion, health information such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center" would clearly come within the constitutionally protected right to privacy.[27]

In a 2011 decision, the Supreme Court held that a state law that prohibited the unauthorized use of prescribing information for marketing purposes by data miners violated their free speech rights under the First Amendment to the Constitution because it allowed others to use the information without comparable restrictions.[28] The data miners in this case purchased the information in de-identified form from pharmacies to help better "detail" sales pitches to physicians. This decision could well mean that privacy laws in the future will have fewer exceptions to the authorization requirements in order to avoid the appearance of discriminating in favor of certain groups.

2. The Right to Privacy in Standards of Professional Ethics

The right to not have one's health information disclosed without one's consent is a core concept of both the Hippocratic Oath and the standards of ethics of "virtually all health professions."[29] The American Medical Association (AMA) has re-affirmed this ethical policy in the context of electronic health information systems:

> "Our AMA policy is that where possible, informed consent should be obtained before personally identifiable health information is used for any purpose."[30]

Medical practitioners can have their licenses suspended or revoked for engaging in unethical conduct. Standards of ethics may also be used in lawsuits for breach of privacy to show that individuals have a reasonable expectation of privacy.

The HIPAA Privacy Rule also provides that even for permitted disclosures, only the "minimum necessary" information may be disclosed to accomplish the purpose of the disclosure, and that this is intended to reflect, be "consistent with, and not override, professional judgment and standards."[31] Professional ethics clearly retain relevance in determining the individual's privacy rights and the potential liability for those who handle protected health information.

3. The Right to Privacy under Federal and State Privileges

The Supreme Court has found, based on the "reason and experience" of the country, that communications between a patient and a psychotherapist, are subject to a "psychotherapist-patient privilege" that can only be waived by the patient.[32] The reason is that effective psychotherapy is completely dependent upon an atmosphere of trust that the therapist will not disclose information that the patient provides in confidence. The psychotherapist-patient privilege recognized at the federal level has also been recognized by all 50 states and the District of Columbia.[33]

At least 43 states recognize a more general physician-patient privilege.[34] The "Privacy" section of the HITECH Act makes clear that nothing in that section is intended to waive any privileges that might otherwise apply.[35] So privileges also remain a source of privacy protection and potential legal liability if they are violated, and mental health information is most likely to be protected under privilege and other privacy laws.

A. Privacy Rights and Liability under Federal Statutes and Regulations

1. HIPAA Privacy and Security Rule and HITECH Act

The HIPAA Privacy and Security regulations prohibit covered entities and their business associates from using or disclosing protected health information except as permitted or required by the HIPAA Privacy Rule.[36] Uses and disclosures are permitted, but not required, for treatment, payment, and health care operation, as well as twelve special purposes.[37] Most other disclosures must be authorized by the individual. "Psychotherapy notes" (notes recorded in any medium by a health care provider who is a mental health professional, documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session, and that are separated from the rest of the individual's medical record)[38] are accorded enhanced privacy protections and cannot be disclosed without patient authorization in most situations.[39]

Under the HITECH Act, covered entities must agree to requests by individuals for restrictions on disclosures of PHI for payment and health care operations if the individual pays out-of-pocket.[40] Failure to comply with these or other restrictions on uses and disclosures is regarded as a violation of the HIPAA Privacy Rule.[41] Covered entities must provide affected individuals, the secretary of HHS, and, in some circumstances, the media, with notice of PHI breaches within statutorily established timeframes.[42] Business associates must notify covered entities of such breaches.[43] Permitted disclosures in most cases are limited to the "minimum necessary" disclosure for the intended purpose.[44] The HIPAA Security Rule establishes nearly 20 standards for protecting the security of "electronic health information," some of which are "required" and some of which are "addressable."[45] When a security standard is addressable, there must be an assessment as to whether it is reasonable and appropriate in the particular environment.[46]

2. Federal Drug and Alcohol Abuse Act

Federal law protecting the confidentiality of alcohol and drug abuse patient records is codified at 42 U.S.C. § 290dd-2 and is better known by its implementing regulation, 42 C.F.R. Part 2. The regulation applies to any federally assisted organization that holds itself out as providing treatment for alcohol or drug abuse, making a diagnosis for that treatment, or making a referral for that treatment.[47] Pre-dating HIPAA by nearly two decades,[48] 42 C.F.R. Part 2 implements stringent confidentiality standards for patient identifying information.[49] 42 C.F.R. Part 2 compliance obligations are unequivocal[50] and violators are liable under the federal criminal code.[51] Potential penalties can be up to $500 for a first offense and up to $5,000 for each subsequent offense.[52]

Organizations that must comply with HIPAA and 42 C.F.R. Part 2 face many challenges regarding information confidentiality.[53] For example, 42 C.F.R. Part 2 pre-empts HIPAA's waiver of patient consent provisions[54] and can significantly narrow what information may be disclosed and re-disclosed about the patient. This becomes a thorny problem in the wake of a data breach, and organizations suffering a breach of patient identifying information may

be liable under both HIPAA's Breach Notification Rule "risk of harm" standard and "impermissible disclosures" under 42 C.F.R. Part 2.[55] Because of this complexity and potential for liability, it has been shown that substance abuse treatment providers are reluctant to hop on the EHR bandwagon.[56]

3. Gramm-Leach-Bliley Act

The *Gramm-Leach-Bliley Financial Modernization Act of 1999* (GLB Act)[57] requires covered companies to give consumers privacy notices that explain the institution's information-sharing practices. The GLB Act applies to "financial institutions," or entities that offer financial products or services to individuals, such as, health or life insurance. Privacy notices must be clear, conspicuous, and accurate statements of the company's privacy practices and include: information the company collects about its consumers and customers, with whom it shares information, and how it protects information. Notices apply to "nonpublic personal information," which includes one's personal information the institution collects in the normal course of business, including social security numbers, account numbers, and financial or health information. Individuals have the right to opt out of having their information shared with certain third parties. Privacy notices must explain how, and offer a reasonable way for them, to opt out; for example, notices can include a detachable form or toll-free telephone number for consumers or customers to use. In addition, privacy notices must explain that customers have a right to say no to the sharing of certain information with the institution's affiliates.

Violations of the GLB Act may result in a civil action being brought by a U.S. attorney. Penalties for violations include: fines upon institutions of up to $100,000 for each violation; fines upon officers/directors of financial institutions of up to $10,000 for each violation; and criminal penalties of imprisonment for up to 5 years, a fine, or both.

4. Genetic Information Non-Discrimination Act (GINA)

The *Genetic Information Non-Discrimination Act of 2008* (GINA)[58] protects Americans against discrimination based on their genetic information with respect to health insurance and employment and includes several health information privacy provisions. If an employer, employment agency, labor organization, or joint labor-management committee obtains genetic information about an employee/member, the information must be maintained on separate forms and in separate medical files. Further, it must be treated as a confidential medical record of the employee/member. The entity may not disclose this information except: (1) to the employee/member at his/her written request; (2) to a health researcher; (3) in response to a court order; (4) to government officials investigating compliance with GINA; (5) to the extent that disclosure is made in connection with the employee's compliance with the *Family and Medical Leave Act of 1993* or similar state laws; and (6) to a federal, state, or local public health agency concerning a contagious disease that presents an imminent hazard.

If violated, individuals may seek reinstatement, hiring, promotion, back pay, injunctive relief, compensatory and punitive damages, and attorney's fees and costs. Plaintiffs may bring suit under the *Employee Retirement Income Security Act* (ERISA) to enforce GINA rights without exhausting administrative remedies after showing that doing so would cause irreparable harm. Courts may order retroactive reinstatements of health coverage and/or penalties of up to $100 per day of noncompliance. Also, the Department of Labor may sue under GINA. Penalties may be up to $100 per day, with minimum penalties of $2,500 for de minimis violations and $15,000 for significant violations. Maximum penalties for unintentional violations are capped at the lesser of 10% of the amount paid by the employer for group health plans during the prior year, or $500,000. Furthermore, there is no cap on the penalty for violations resulting from case-law defined willful neglect[59] or intentional misconduct.[60]

5. Family Educational Rights and Privacy Act

The *Family Educational Rights and Privacy Act of 1974* (FERPA)[61] protects the privacy of student education records and applies to all schools (including student health clinics at colleges and universities) receiving funds under an applicable program of the U.S. Department of Education. These records may include health information such as medications taken and/or immunization records. If a person or entity acting on behalf of a school subject to FERPA (such as a school nurse) directly maintains student health records, these records are education records under FERPA. As education records, the information is protected under FERPA and not HIPAA.

FERPA gives parents certain rights with respect to their children's education records. These rights then transfer to students when they reach the age of 18 or attend post-secondary institutions. Students to whom the rights have transferred are "eligible students." Schools must have written permission from the parent or eligible student to release any information from the student's education record. However, records may be released without consent to certain entities and in certain situations, including: to school officials with legitimate educational interest; other schools to which a student is transferring; specified officials for audit or evaluation purposes; appropriate parties in connection with financial aid to a student; organizations conducting certain studies for or on behalf of the school; accrediting organizations; to comply with a judicial order or lawfully issued subpoena; appropriate officials in cases of health and safety emergencies; and state and local authorities, within a juvenile justice system, pursuant to specific state law.

The Family Policy Compliance Office reviews and investigates complaints of violations of FERPA. Penalties can include the withdrawal of Department of Education funds. Courts routinely hold that FERPA does not create a private right of action against the educational institution.

B. Privacy Rights and Liability under State Statutes and Regulations

While the HIPAA Privacy and Security Rules are the most generally applicable requirements concerning an individual's health information, state laws also create health information privacy rights and obligations. In enacting HIPAA, Congress established a federal "floor" of privacy protections allowing for more restrictive privacy protections under state regimes to remain in effect.[62]

HIPAA provides that only state laws that are contrary to the provisions or requirements of the HIPAA Privacy Rule are pre-empted by the federal requirements and that contrary provisions of state law that confer "more stringent" privacy protections are not superseded.[63] California has the most stringent patient privacy laws in the nation – stronger than the federal laws.[64] Therefore, a covered entity – and particularly one with operations across numerous states – should pay careful attention to the requirements of state laws to ensure compliance with applicable federal and state law. Health care organizations sometimes mistakenly believe that if they are in compliance with the federal HIPAA Privacy and Security Rules, they are also in compliance with state privacy laws.

As of October 2010, 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands had enacted electronic data breach disclosure laws.[65] Some of these laws require notice of data breaches that are not required under the HITECH Act's breach notice provisions. Organizations should check these laws as well as the federal breach notice laws to ensure that they are in compliance with both in the case of an information breach.

With some exceptions, such as California's *Confidentiality of Medical Information Act,* states have not instituted broad privacy requirements concerning health information. A few states and territories (Minnesota, New York, Vermont, Puerto Rico, and Guam) have privacy protections that require patient consent for disclosures by hospitals to other providers. Other states either adopt the HIPAA Privacy Rule protections or allow disclosures as permitted by law.

Congress mandated in the HITECH Act that the HIT Policy Committee, which was established under that Act, make recommendations to Congress for technologies to protect the privacy of "sensitive individually identifiable health information" including "segmentation" of such information.[66] No such recommendations had been made as of October 2011 but the HHS Office of the National Coordinator had begun an information gathering exercise.

C. Privacy Rights under Tort and Contract Laws in the States and District of Columbia

Most states and the District of Columbia recognize in case law the torts of invasion of privacy and intrusion upon seclusion that would be offensive to the reasonable person. The common law in some states recognizes a right to health information privacy as part of an implied contract between patients and their health care providers.[67] The application of these laws in any given case may be hard to assess. Additionally, tort theories traditionally have as an element some measure of damages. Outside of any alleged mental anguish type damages, if one does not suffer actual monetary damages, the reach of state tort law to provide redress is somewhat of an open issue. However, there are new damages theories that are being advanced based upon the "value" of the information to an individual.[68] When actual out-of-pocket damages are suffered (for example, where one expends time and/or money to repair their health information records after medical identity theft), law suits based on tort theories may provide redress.

ENDNOTES

[1] "Breaches Affecting 500 or More Individuals." United States Department of Health and Human Services. Web. 31 Jan. 2012. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html.

[2] New London Consulting. How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes. Rep. 13 Sept. 2011. FairWarning. Web. http://www.fairwarning.com/documents/2011-WHITEPAPER-US-PATIENT-SURVEY.pdf.

[3] HHS finding, 65 Fed. Reg. at 82,776 (Dec. 28. 2000).

[4] Ponemon Institute LLC. "2010 Annual Study: U.S. Cost of a Data Breach." Sponsored by Symantec Corporation, March 2011. Web. http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach; ID Experts. "Data Breaches Cost the Healthcare Industry an Estimated $6.5 Billion; Latest Ponemon Study Reveals Data Breaches Up 32 Percent Due to Sloppy Mistakes and Unsecured Mobile Devices." December 1, 2011. Web. http://www2.idexpertscorp.com/press/healthcare-news/data-breaches-cost-the-healthcare-industry-an-estimated-65-billion/

[5] U.S. Department of Health and Human Services. HHS Imposes a $4.3 Million Civil Money Penalty for Violations of the HIPAA Privacy Rule. HHS.gov, 22 Feb. 2011. Web. http://www.hhs.gov/news/press/2011pres/02/20110222a.html.

[6] U.S. Department of Health and Human Services. "Massachusetts General Hospital Settles Potential HIPAA Violations." HHS.gov, 24 Feb. 2011. Web. http://www.hhs.gov/news/press/2011pres/02/20110224b.html.

[7] U.S. Department of Health and Human Services. "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities." HHS.gov, 7 July 2011. Web. http://www.hhs.gov/news/press/2011pres/07/20110707a.html; Conn, Joseph. "UCLA Health System Agrees to Settle HIPAA Complaints." ModernHealthcare.com. 7 July 2011. Web. http://www.modernhealthcare.com/article/20110707/NEWS/307079962.

[8] Simpson, Elizabeth. "Suffolk Doctor Faces Federal Privacy Law Charges." PilotOnline.com. The Virginian Pilot, 23 June 2011. Web. http://hamptonroads.com/2011/06/suffolk-doctor-faces-federal-privacy-law-charges.

[9] Anderson, Howard. "10.8 Million Affected by Major Breaches." GovInfoSecurity.com. 25 Apr. 2011. Web. http://www.govinfosecurity.com/articles.php?art_id=3576.

[10] "Times Staff Report." Ind. AG Reaches Settlement with WellPoint in Consumer Data Breach." Nwitimes.com. Northwest Indiana Times, 5 July 2011. Web. http://www.nwitimes.com/business/local/article_7feddb17-aa1c-5950-b743-cec018b84267.html.

[11] Nicastro, Dom. "HIPAA Faces HITECH-Empowered State AGs." HealthLeaders Media, 27 July 2010. Web. http://www.healthleadersmedia.com/page-1/LED-254310/HIPAA-Faces-HITECHEmpowered-State-AGs.

[12] Mosquera, Mary. "HHS Taps KPMG to Perform HIPAA Audits." Government Health IT. 6 July 2011. Web. http://www.govhealthit.com/news/hhs-taps-kpmg-perform-hipaa-audits.

[13] Office of the Inspector General. Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight. Rep. U.S. Department of Health and Human Services, 16 May 2011. Web. http://www.workplaceprivacyreport.com/uploads/file/Office%20of%20Insp%20Gen%20Re%20HIPAA%20enforce%205-16-11.pdf.

[14] Yen, Hope. "VA Agrees to Pay $20 Million to Veterans in 2006 Data Breach." Boston.com. The Boston Globe, 28 Jan. 2009. Web. http://articles.boston.com/2009-01-28/news/29254594_1_data-theft-veterans-groups-va-inspector.

[15] BNA. "LensCrafters, Pearle Settle Class Actions Alleging Consumer, Privacy Law Violations." Health Care Daily, 15 Aug. 2008.

[16] Vijayan, Jaikumar. "Defense Dept. Hit with $4.9B Lawsuit over Data Breach." Computerworld. 14 Oct. 2011. Web. http://www.computerworld.com/s/article/9220874/Defense_Dept._hit_with_4.9B_lawsuit_over_data_breach.

[17] Redhead, C. Stephen. Rep. The Health Information Technology for Economic and Clinical Health (HITECH) Act. Congressional Research Service, 23 Feb. 2009. Web. http://www.nationalehealth.org/sites/default/files/hitech_act.pdf.

[18] Id. at p. 1; Jha, Ashish K., and Catherine M. DesRoches, et al. "Use of Electronic Health Records in U.S. Hospitals." The New England Journal of Medicine. 16 Apr. 2009. Web. http://www.nejm.org/doi/full/10.1056/NEJMsa0900592#t=article.

[19] 65 Fed. Reg. at 82,467 (Dec. 28, 2000).

[20] Id.

[21] Id.

[22] Freudenheim, Milt. "Breaches Lead to Push to Protect Medical Data." Nytimes.com. The New York Times, 30 May 2011. Web. http://www.nytimes.com/2011/05/31/business/31privacy.html?pagewanted=all.

[23] Citizens for Health v. Leavitt, 428 F.3d 167, 177 (3rd Cir. 2005), cert. den. 127 S. Ct. 43 (2006).

[24] Bivens v. Six Unknown Fed. Narcotic Agents, 403 U.S. 388, 91 S. Ct. 1999 (1971).

[25] Gruenke v. Seip, 225 F.3d 290 (3rd Cir. 2000).

[26] Sterling v. Borough of Minersville, 232 F.3d 190 (3rd Cir. 2000).

[27] United States v. Jones, ___S. Ct. __, 2012 WL 171117 (Jan. 23, 2012).

[28] Sorrell v. IMS Health, Inc., 564 U.S. _, 131 S. Ct. 2653 (2011).

[29] National Committee on Vital and Health Statistics. Privacy and Confidentiality in the Nationwide Health Information Network. Rep. U.S. Department of Health and Human Services, 22 June 2006. Web. http://ncvhs.hhs.gov/060622lt.htm.

[30] American Medical Association, Report 19 of the Board of Trustees (A-07), Patient Information in the Electronic Medical Record.

[31] 67 Fed. Reg. at 53,1973; 65 Fed. Reg. at 82,544.

[32] Jaffee v. Redmond, 518 U.S. 1, 116 S. Ct. 1923 (1996).

[33] See statutes cited in Jaffee v. Redmond, 518 U.S. 1, 12, n. 11, 116 S. Ct. 1923 (1996).

[34] Pritts, Joy, and Angela Choy, et al. State of Health Privacy: A Survey of State Health Privacy Statutes. Rep. 2nd ed. Washington: Institute for Health Care Research and Policy at Georgetown University, 2002. Health Privacy Project. The Robert Wood Johnson Foundation, June 2002. Web. http://ihcrp.georgetown.edu/privacy/pdfs/statereport1.pdf.

[35] 42 U.S.C. § 17951(c); HITECH Act, section 13421(c).

[36] 45 C.F.R. § 164.501, et seq.; 45 C.F.R. § 164.302 et seq.

[37] 45 C.F.R. § 164.502; 164.512.

[38] 45 C.F.R.§ 164.501 Definitions.

[39] 45 C.F.R. § 164.508(a)(2).

[40] 42 U.S.C. § 17935(a); HITECH Act, section 13405(a).

[41] 45 C.F.R. § 164.522(a)(1)(iii).

[42] 42 U.S.C. § 17932; HITECH Act, section 13402.

[43] 42 U.S.C. § 17932(b); HITECH Act, section 13402(b).

[44] 45 C.F.R. § 164.514(d).

[45] 45 C.F.R. § 164.306-316.

[46] 454 C.F.R. § 164.306(d).

[47] 42 C.F.R. § 2.11.

[48] Ms. Rose Jade is a noted authority on the history of 42 C.F.R. Part 2. See: Jade, Rose. "The Secret Life of 42 CFR Part 2 - What Every Defender and Investigator Needs to Know About Patient Records from Federally Funded Drug or Alcohol Treatment Centers." The Champion, Vol. 30, No. 34, April 2006. Available at SSRN: http://ssrn.com/abstract=1128955.

[49] 42 C.F.R. § 2.11.

[50] 42 C.F.R. § 2.13(b).

[51] 42 U.S.C. § 290dd-2(f).

[52] 42 U.S.C. § 17939(d); HITECH Act, section 13410(d).

[53] Substance Abuse and Mental Health Services Administration and the U.S. Department of Health and Human Services. The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs. Rep. Substance Abuse and Mental Health Services Administration, June 2004. Web. http://www.samhsa.gov/HealthPrivacy/docs/SAMHSAPart2-HIPAAComparison2004.pdf.

[54] Ibid. p. 5.

[55] "Breach Notification for Unsecured Protected Health Information; Interim Final Rule." 74 Federal Register 162 (August 24, 2009), footnote 8 p. 42745.

[56] Legal Action Center. "Confidentiality of Alcohol and Drug Records in the 21st Century." Jan. 2010. Web. http://www.lac.org/doc_library/lac/publications/Confidentiality_of_Alcohol_and_Drug_Records_in_the_21st_Century-1-20-10.pdf.

[57] Pub.L. 106-102, 113 Stat. 1338 (Nov. 12, 1999).

[58] Pub.L. 110-233, 122 Stat. 881 (May 21, 2008).

[59] Willful neglect has been defined as a "conscious, intentional failure or reckless indifference." "Whether a failure to file timely is due to reasonable cause and not willful neglect is a question of fact." Cunningham v. Comm'r, T.C. Memo 2009-194 (T.C. 2009).

[60] The term "intentional misconduct" means conduct by a person with knowledge (at the time of the conduct) that the conduct is harmful to the health or well-being of another person [42 USCS § 1791 (b) (8)].

[61] Pub. L. No. 93-380 (1974).

[62] 67 Fed. Reg. at 53,212.

[63] 42 U.S.C. § 1320d-2(c)(2); HIPAA, section 264(c)(2).

[64] Nicastro, Dom. "Beware of More Stringent State HIPAA Laws." HealthLeaders Media, 24 July 2009. Web. http://www.healthleadersmedia.com/content/TEC-236461/Beware-of-More-Stringent-State-HIPAA-Laws.html.

[65] National Conference of State Legislatures. "State Security Breach Notification Laws." NCSL.org. 6 Feb. 2012. Web. http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

[66] 42 U.S.C. § 300jj-12(b)(2)(B); HITECH Act, section 3002(b)(2)(B).

[67] Givens v. Millikin, 75 S. W. 3d 383 (Tenn. 2002).

[68] Manos, Diana. "Patients Sue Walgreens for Making Money on Their Data." Healthcare IT News. 18 Mar. 2011. Web. http://www.healthcareitnews.com/news/patients-sue-walgreens-making-money-their-data; Kramer, Reuben. "CVS Faces Suit for Prescription Data Sales." Courthouse News Service. 8 Mar. 2011. Web. http://www.courthousenews.com/2011/03/08/34749.htm.

APPENDIX C

Legal Considerations with Respect to Cloud Computing

Cloud computing is not governed by statutes or regulations unique to the cloud nor unique to health data processed or stored in a cloud infrastructure. However, cloud computing presents heightened opportunities for breaches of protected health information (PHI) because of the nature of the infrastructure itself, and because of the complexities that the infrastructure creates in securing satisfactory contractual arrangements with a provider of cloud services.

In cloud computing, the entity purchasing cloud computing services, i.e., the "consumer" or "user," contracts with a cloud provider to access its resources – hardware infrastructure, software, and data storage, for example – on a dynamic, on-demand basis. How much service and where the service or the consumer's data will be located are not always known at the time of the contract, as services and processing power may be located in a number of sites including several countries.

Cloud computing is somewhat similar to a shared utility or a shared facility. Each user is responsible for preparing the resources to suit its own needs for data protection. The cloud provider's resources are shared among all consumers dynamically so that as one user finishes a task, removes his software or data, or relinquishes control of a resource, another user's software and data may move in to consume that same resource. The high speed and frequent swapping of consumers and resources create opportunities to lose control if not very carefully managed by the user and the cloud provider.

Cloud computing presents heightened opportunities for PHI breaches because of the nature of the infrastructure.

Although a cloud services environment can be created by a consumer and controlled internally in a private cloud for sharing computing resources within an organization, there are a number of issues that a consumer must consider in purchasing public cloud services (or even a hybrid public and private cloud). While sharing resources hosted internally in a private cloud requires that the entity address many of the same regulatory access and control issues that exist in a public cloud, with a private cloud the organization has more control over its data among its own users. Less consumer control may exist in a public cloud setting, and possibly in a hybrid cloud, depending on the cloud provider's ability and willingness to accommodate consumer-unique needs and on specifying expectations in the contractual arrangements.

As with other "traditional" outsourcing arrangements, when the consumer of cloud services is a HIPAA- *(Health Insurance Portability and Accountability Act of 1996)* covered entity that contracts for computing services and the services include handling of PHI, it is probably prudent to require a business associate agreement (BAA) with the cloud provider. (This is in addition to the service level agreement [SLA] or contract for performance between the parties.) The full slate of federal protections, required and mandatory, apply to PHI stored or processed in an outsourced cloud environment. Access to the PHI must be controlled and must be limited to the "minimum necessary" data fields required for the purpose involved.

Both the covered entity and the cloud provider may be subject to federal civil penalties for a breach of PHI.

Limiting access to only the "minimum necessary" data entails having the means to allow access only to authenticated and authorized users; to log and audit all accesses; and to provide a patient with information about accesses/disclosures upon request, for example. Many states have similar or more stringent access controls on health information as well. Further, as federal and/or state protections of personally identifiable information including PHI change over time, the consumer and cloud provider must have the means to adjust to comply with new or revised rules.

Ultimately, the consumer of the cloud services retains full legal responsibility for compliance with any applicable statutes and regulations. The consumer that is a covered entity does not transfer its accountability to a contractor providing services. While a covered entity buying cloud services may be able to sue the cloud provider for breach of contract in the event of an unauthorized disclosure of PHI or breach of other terms in the SLA and/or BAA or performance contract, both the covered entity and the cloud provider may be subject to federal civil penalties for a breach of PHI under HIPAA and/or state regulations. The covered entity must ensure that it can manage the protection of its sensitive data in a cloud processing configuration, just as it must ensure it can protect such data in its own environment.

APPENDIX D

PHI Threat Scenarios

The evolving health care ecosystem is comprised of those responsible for safeguarding protected health information (PHI) from five major stakeholder groups: points of care, payers, clinical support, business associates, and other entities. IT services, both within organizations and as an ancillary support, provide the technology and infrastructure to drive the electronic health record system for all stakeholders.

PHI data is at risk while at rest and as it flows throughout the ecosystem from stakeholder to stakeholder. To demonstrate PHI vulnerabilities and risk points within the ecosystem, health care professionals involved in the PHI project, and representing each stakeholder group, collected and compiled details from over 40 recent breaches and categorized them into a list of eleven elements that threaten PHI security.

These eleven "PHI Threat Scenarios" are described in greater detail in this appendix. The scenarios use fictitious names and places but are based on actual PHI security breaches. Threat Scenario #7 (Business Associates, Suppliers, Vendors, and Partners) was used to develop the breach-costing scenario found in Chapter 8 of the report.

Health care executives should require that their staff clearly understand the potential threats and risks to their organization.

For each of the scenarios, the reader is invited to ask him- or herself: Can this happen in my organization? What can we do to prevent a security breach or detect the breach before significant harm is done? What are the reputational, financial, legal/regulatory, operational, and clinical repercussions to the organization if we don't implement the necessary safeguards and controls? To facilitate the reader's analysis, preventive measures based on policy, procedures, and technology are enumerated for each scenario.

Health care executives should require that their staff clearly understand the potential threats and risks to their organization, as well as the preventive measures that may be required to mitigate these risks. The successful security professional will use this information to help justify the cost of implementing appropriate safeguards and controls as part of a business case for enhanced PHI security.

PHI Threat Scenario #1: Malicious Insider

Medical identities can be used to receive fraudulent medical care for months before being detected.

Malicious insider threats represent a significant risk to stakeholders in the healthcare ecosystem. According to a 2010 Data Breach Investigations Report, insiders were responsible for almost half of all breaches occurring that year, an increase of 26 percent from the year before. The insider's elevated privileges and knowledge of control measures may allow the bypassing of physical and logical security measures designed to prevent, detect, or react to unauthorized access. (Source: Verizon RISK Team's 2010 Data Breach Investigations Report conducted in cooperation with the U.S. Secret Service.)

In this scenario, the malicious insider was a system administrator who sought revenge after being fired from his position at a small claims payer.

A large health care provider across town was using the claims payer to send, receive, and process their HMO medical billing information and Medicaid claims in an effort to reduce paper usage and save printing costs. Routinely, PHI was being transferred between the health care provider and claims payer through an electronic data exchange in a password-protected encrypted file. The payer placed processed claims records on the health care provider's file transfer protocol (FTP) site where they could copy the file to retrieve the records.

The fired system administrator was familiar with this routine procedure. He also knew that his former employer did not always change encryption passwords after personnel changes and that it took at least 30 days for remote access to the system to be eliminated. With the payer's administrative password still in his possession, he was monitoring the FTP site from his home, logging on every night after midnight when remote access channels were typically not being observed.

Eventually, he found a new set of encrypted claims files transferred by the payer to the health care provider's FTP site. Using the old administrative password, he copied the encrypted files to his desktop, easily breaking the five-character password with a commonly used hacker program available on the Internet. He discovered a cache of over a thousand claims records containing full patient profiles: name, address, social security number (SSN), date of birth, medical record number, health plan beneficiary numbers, and credit card account numbers.

From a fraudster's perspective, medical identities have a much longer shelf life than credit cards. They can be used to receive medical care costing tens or even hundreds of thousands of dollars, and transactions can go undetected for months. The system administrator had been chatting with bloggers on a black market card reader forum that regularly advertised the value of stolen PHI. He knew what other members of the forum were eager to buy and for what price. Minutes after downloading the health care provider's claims file from the FTP site, the administrator posted the stolen PHI records for sale on the card reader forum at $125 each.

The records sold fast — and within months, the reputation of the health care provider and the personal lives of the provider's 1,500 customers, residents of Laguna Woods, a wealthy California retirement community, were impacted like never before.

Patients began receiving invoices for pharmaceuticals never ordered and treatments never received. Many reported the fraudulent activity to the health care provider who discovered the PHI breach and posted a notice. The breach was reported to the local news, creating a firestorm in the community.

Law enforcement officers and private Internet security experts traced the blog posting of PHI records for sale back to a server used by the system administrator via his URL address, linking him to the stolen PHI. The system administrator was arrested and prosecuted for ID theft. The payer's CEO resigned and the head of IT was fired. A full time security officer was hired who committed to implementing encryption across the payer's network.

Preventive Measures

Policy:

1. Immediate change of encryption passwords and termination of employee's remote access when fired or leaving the organization.
2. Implementation of strong passwords by all employees.

Procedures:

1. Implementation of a strong security awareness program focused on the importance of maintaining a secure environment for the organization.
   a. Notification to all employees on the new procedure for termination of remote access and encryption password changes immediately after employee departure for any reason.
   b. Notification to all employees on mandated implementation of stronger passwords: more than six characters and a combination of mixed characters, symbols, numbers.
1. Strong enforcement practices for failing to adhere to the organization's policies.

Technology:

1. Implementation of a more secure FTP.

PHI Threat Scenario #2: Non-Malicious Insider

Because the non-malicious insider threat is most often attributable to "human error," it is often the hardest to prevent.

In this scenario, a payer had implemented, without testing, an application programming change that affected users' access to explanation of benefits (EOB) statements online using the insurance carrier's secure website. An undetected programming error resulted in cross-site scripting, allowing a young man to view the EOB statement of another patient.

The other patient was the city's mayor, a politician the young man did not particularly like. The mayor's EOB statement outlined details of his last doctor's visit, prescribed detoxification treatments for his drug and alcohol abuse, and medications to help the mayor overcome his addiction to Xanax. The young man printed out the mayor's EOB and submitted it to the local news office. The local press ran the story about the mayor's drug problem and the story was picked up by national news. The reputation of the mayor was ruined and he was forced to step down from his position.

Investigators traced the PHI breach back to the payer's website and online EOB access when the press published details of how the mayor's struggle with drug addiction was initially discovered.

Preventive Measures

Policy:

1. Establishment of appropriate quality assurance (QA) policies for new application development.
2. Separation of duties (QA and programming staff).

Procedures:

1. Implementation of a strong security awareness program focused on the importance of maintaining a secure environment for the organization.
2. New application code reviews, quality control, post implementation testing, and monitoring.
3. Strong enforcement practices for failing to adhere to the organization's policies.

PHI Threat Scenario #3: Outsider

The outsider threat is someone who has no formal relationship to the company and does not have authorized access to its data. In 2009, the majority of breaches and almost all data stolen was the work of criminals outside the victim's organization. (Source: Verizon RISK Team's 2010 Data Breach Investigations Report conducted in cooperation with the U.S. Secret Service.)

In this scenario, a vendor visited a medical laboratory to give a presentation. When the lab's in-house presentation equipment failed, and IT support was unavailable to resolve the problem, the lab staff decided to override established security protocols and allow the vendor to use her personal laptop to connect to the medical laboratory's network.

The lab's network anti-virus updates were not updated automatically and a Virus/Trojan on the vendor's device infected the lab's network, accessing and copying the lab's database of 10,000 patient records. At the next Internet connection, the vendor's device sent the patient files to hackers.

When lab users could not access the mail server, and system performance of other applications was notably affected, the IT department was notified. A firewall report revealed an unauthorized device had accessed the network. The lab's visitor sign-in sheet led the IT investigation back to the vendor presentation earlier that day. Further investigation revealed mis-configured software and out-of-date virus configurations on the network, which allowed the vendor's network connection to deliver the virus to the system.

The lab sent a notification to all impacted patients outlining the breach, the PHI exposed, and who handled the data. The breach was leaked to the media who ran a story in the local press. The lab sent subsequent letters to all impacted patients after the story ran in the news. The lab suffered a loss of goodwill, as well as a damaged brand name, among its constituents. Management was fired and an internal study was conducted on how to mitigate a similar risk of breach in the future.

Preventive Measures

Policy:

1. A new policy prohibiting non-company owned and controlled devices being attached to the organization's network.
2. Automated updates of network virus prevention.

Procedures:

1. Implementation of a strong security awareness program focused on the importance of maintaining a secure environment for the organization.
2. Procedures relating to the ban on outsider-owned and controlled devices attaching to the organization's network.
3. Procedures for automated virus control updates.
4. Strong enforcement practices for failing to adhere to the organization's policies.

Technology:

1. Automatic antivirus updates.
2. Logically separate network traffic from non-organizational devices to prevent access to the broader organizational network.
3. Data leakage prevention (DLP) technology to stop PHI from being sent out of the internal network.

PHI Threat Scenario #4: Lost / Stolen Media

An unattended company laptop containing 46,000 PHI records was stolen and the records were sold on the black market.

In a European survey conducted by the Ponemon Institute, researchers determined that the costs to organizations as a result of lost or stolen laptops was $49,256 per device, or a combined cost of $6.4 million per organization on average. Two industry segments experienced the highest rate of laptop loss overall — education and research, and health and pharmaceutical. (Source: Ponemon Institute Survey, "The Billion Euro Lost Laptop Problem," released 4/2/10.)

In this breach scenario, an unauthorized person(s) seized an opportunity to gain physical access to the administrative area and accounts payable office of a mental health agency when they found a door from the back room to an alleyway propped open for better air flow on a hot day.

An unattended company laptop was stolen from a desk and never recovered. The laptop contained 46,000 PHI records belonging to approximately 15,000 mental health patients including names and addresses, policy ID numbers, medical provider names and addresses, medical diagnoses, conditions, treatments, cyber breach database codes, dates of service, diagnostic codes, procedure names and codes, and a comment field in some of the records meant to hold notes justifying the procedures.

The thief sold the stolen laptop on the street for $150. The 46,000 PHI records on the laptop were sold on the black market for over $10,000.

The mental health agency notified the state's attorney general's office of the breach and posted a public notice. All affected individuals were sent letters of notification. Credit monitoring and other risk consulting services were offered to affected individuals for one year. Credit restoration and identity theft insurance was offered to affected individuals if needed.

Preventive Measures

Policy:

1. Physical security policies that require all doors to be locked and/or attended to prevent unauthorized access.
2. Policies requiring all laptops to have full encryption automatically implemented.
3. Strong information classification and handling policy.

Procedures:

1. Implementation of a strong security awareness program focused on the importance of maintaining a secure environment for the organization.
2. Implementation and monitoring of physical and logical security controls to prevent someone from opening a door and leaving a laptop unattended.
3. Implementation of full encryption on all mobile devices.
4. Strong enforcement practices for failing to adhere to the organization's policies.

Technology:

1. Alarm for open door and CCTV monitoring.
2. Transparent encryption technology.

PHI Threat Scenario #5: Dissemination of Data

There are many stakeholders within the health care ecosystem, and PHI data flows to and from them regularly. Weak technology and security controls allow for the easy breach of PHI during its daily dissemination.

In this scenario, a disease management association was asked to provide a university research department with data for a diabetic study. There was no Business Partner Trading Agreement in place, and the data file for the research study was created from a standard output report template. The PHI fields were not removed. No audit of the data file was done prior to sending. Consumer identifying information was not removed.

As a result of these oversights, the university received over 6,000 PHI records of diabetic patients (name, diagnosis, and a portion of their member information). A university lab employee determined that the data would not be traced back to university and decided to sell the PHI.

Once the breach was reported, the disease management association notified all impacted patients, outlining the free services they promised to provide should any fraudulent uses of their identity occur. The local media ran a story on the breach, which resulted in additional lawsuits and legal fees as well as the loss of goodwill among the association's constituents.

Preventive Measures

Policy:

1. Policy requiring a contract governing all outside engagements and relationships.
2. Policy requiring the removal of all sensitive information from files superfluous to the business purpose.
3. Quality control policy that requires oversight of all external file transfers.

Procedures:

1. Implementation of a strong security awareness program focused on the importance of maintaining a secure environment for the organization.
2. An auditing process ensuring that the format of shared data complies with the PHI Privacy Rule, and all PHI identifying data is removed prior to transmission.
3. Strong enforcement practices for failing to adhere to the organization's policies.

PHI Threat Scenario #5: Mobile Devices

Mobile devices such as PDAs and tablets are quickly gaining acceptance. Ubiquitous across the health care ecosystem, they pose a growing threat to PHI.

In this scenario, a health care provider hired a new IT executive who bypassed the normal procurement process for digital devices, buying an iPad for his business use based on his signing authority. The executive downloaded his emails to the iPad and received a large file of health care patient records as part of his group's work on the system.

Later, the IT executive inadvertently left his iPad behind in a restaurant where it was stolen. Subsequent investigation found that there were over 100,000 patient records on the system containing all forms of PHI including patient names, addresses, SSNs, drivers license numbers, birth dates, Medicare numbers, medical records and patient history, patient treatment plans, lab results, doctors' comments, and children's names, address and medical history.

The PHI on the lost iPad was later used by individuals to fraudulently receive health care.

Preventive Measures

Policy:

1. Require that all individuals be responsible for adherence to policies regardless of job title.
2. Policy to govern the use of mobile devices.

Procedures:

1. Implementation of a strong security awareness program focused on the importance of maintaining a secure environment for the organization.
2. Implementation of a protective procedure for the purchase and use of mobile devices.
3. Strong enforcement practices for failing to adhere to the organization's policies.

Technology:

1. Mobile device security prevention and detection technologies such as virus/malware protection.
2. Data Leakage Prevention technology to detect that PHI is being sent unencrypted via email.

PHI Threat Scenario #7: Business Associates, Suppliers, Vendors, and Partners

According to HIPAA guidelines, the health care ecosystem stakeholder must include certain protections for PHI in a Business Associate Agreement when outsourcing the services of business associates, suppliers, vendors, and partners who handle, use or disclose PHI. All legal and financial repercussions associated with a PHI/PII data breach caused by such third parties are the responsibility of the health care ecosystem stakeholder. The liability to the health care ecosystem stakeholder for failing to maintain proper due diligence in terms of data security cannot be overestimated. There are severe financial, regulatory and reputational repercussions for not managing these relationships. (Source: HIPAA Security Final Rule – 45 C.F.R. §164.308 Administrative Safeguards, – 45 C.F.R. §164.314 Organizational Requirements, – 45 C.F.R. §164.504 Uses and Disclosures: Organizational Requirements.)

In this scenario, a major New York City hospital server housing a database of over 845,000 patient records could no longer be accessed due to the mechanical failure of the hard drives. The IT manager followed procedures to restore the database from the hospital's magnetic backup tapes, but the backup tapes were blank.

The permanent loss of the database records would put the hospital in clear violation of HIPAA data retention and availability requirements. To restore the server, the IT manager contracted with a local third-party data recovery service provider. With no documented policy or procedure for assessing the capabilities and security compliance of such service providers, the IT support manager selected the company based on their 48-hour turnaround time, and shipped them the damaged hard drives without vetting their data security protocols.

The data recovery was a complete success. Within two days, the recovered data was returned to the IT support manager who uploaded the full database of patient records onto the hospital's new server and the tape backup system was fully functional again. The IT manager made a note in his files to use the local data recovery service provider again, thinking all had gone quite well.

But all was not well. Several months after the recovery, the hospital discovered that a breach of PHI had occurred during the recovery process. While creating an image of all the data on the drives, the data recovery engineer discovered the database of PHI records, including financial and health care account information. He made a second copy of the database for himself, found the records of a female patient with a description closely matching that of his ailing wife, and altered them to fit his wife's description perfectly, removing references to the female's blood type and life-threatening allergy to insulin. His wife used the fraudulent identity to receive surgical treatments for cancerous tumors in her lungs. The engineer used the credit card data found in other records to pay for the surgery, pharmaceuticals, and rehabilitation.

After a breach of hospital records, patients' PHI was misused and the hospital's image was damaged severely.

Several of the hospital's patients began reporting unauthorized purchases on their credit cards. The cause of the security breach was not discovered until the woman whose record was altered received emergency surgery after a car crash. Unconscious when she arrived at the hospital, she died from anaphylactic shock during a simple surgical procedure – an allergic reaction to the insulin she was administered during the operation.

The husband was convinced that his wife's allergy to insulin was well documented in her health record. After investigating the woman's health records more closely, it was discovered that her PHI recently had been altered and the changes were traced back to the NYC hospital's database. The hospital's forensic team was called in, and the breach was traced to the third-party data recovery service provider and their unscrupulous data recovery engineer, who, it was then revealed, had not been subjected to a background check upon hiring. The data recovery engineer had a criminal history of identity theft.

Reports of the breach, the altered medical records, and the woman's death were picked up by the media. The hospital posted a public notice of the PHI breach and notification letters were sent to all impacted patients outlining the details of the breach, the PHI disclosed, and who had handled their data. Two years of credit monitoring and fraud resolution services, along with credit and identity theft restoration if needed, were offered by the hospital to all affected individuals. However, the larger threat to the patients was the misuse of their PHI which had gone unmonitored. The hospital's brand name and image were damaged severely.

An internal study was conducted at the hospital and new protocols were adopted to mitigate the risk of using third-party data recovery vendors. The hospital's risk management process was updated and the hospital's chief information security officer (CISO) and the IT support manager were fired.

Preventive Measures

Policy:

1. Vetting guidelines that include: third-party verification of the service provider's data security protocols; proof of compliance with HIPAA/HITECH data privacy/protection guidelines; certification of a secure network; background checks on all employees who handle drives and data during the recovery process; training of recovery engineers to safely manage encryption keys; non-disclosure agreements; and chain-of-custody protocols.
2. All business associates are evaluated by the covered entity's vendor risk assessment program and include a full security program review.
3. Mandatory update of security reviews of business associates at least annually.

Procedures:

1. Defined, documented and repeatable business-associate risk management processes.
2. At least an annual review of business associate security practices.
3. Strong enforcement practices for failing to adhere to the organization's policies.

PHI Threat Scenario #8: Cloud Computing Providers

Cloud computing providers create security risks to health care ecosystem stakeholders in many areas, such as data integrity, recovery, and privacy, e-discovery, regulatory compliance, and auditing.

In this scenario, a health care CFO, trying to save money for his facility, moved a system with PHI over to an outsourced cloud computing provider. The health care provider had no policy or enforcement in place that called for legal or security to review and vet the third party prior to outsourcing.

The cloud computing provider was not aware of the regulatory requirements for protecting PHI information. It suffered a security breach and all forms of PHI were lost, including patient records, patient treatment plans, lab results, doctors' comments, and patients' personal information such as SSNs, drivers license numbers, etc. The cloud computing provider was unable to provide proper forensics information or meet legal discovery demands.

The breached health care information of a prominent patient was published in the media, leading to public embarrassment and a law suit.

The breached patient information was used to perform identity theft and medical identity theft. The health care information of one prominent patient was published in the media, leading to public embarrassment when her medical condition was exposed.

The health care provider suffered legal penalties, regulatory fines, and it was required to disclose the breach to patients. The reputational damage was severe, resulting in the loss of customers and partners. Increased fines were imposed because of lack of compliance with discovery law. Legal suits are ongoing as well as regulatory sanctions and oversight.

Preventive Measures

Policy:

1. Planning and development of a robust cloud risk management strategy.
2. Update vendor risk assessment program to include a full security program review and vendor vetting guidelines for all business associates who handle PHI, including cloud computing providers.
3. A policy requiring that due-diligence is completed on cloud computing providers prior to engaging their services.

Procedures:

1. Due-diligence procedures with additional attention to the contract requirements, discovery and forensics processes, and the exit strategy when moving to another provider.
2. Audits of the cloud provider's business continuity and disaster recovery processes, the physical security of any hosting facility it uses, tactics to secure the core network and remote network links into your network, as well as how it will protect its servers and storage and your encrypted data.
3. Strong enforcement practices for failing to adhere to the organization's policies.

PHI Threat Scenario #9: Virtual Physician's Office

Physicians may provide home care and procedures for patients who have conditions that inhibit their ability to visit the doctor without assistance. These physicians often lack the resources to appropriately manage data security and, yet, as health care providers, they are expected to comply with rather complex standards.

When a car was stolen, a laptop and health care monitoring device inside were accessed by the thief and PHI was used to commit identity theft.

In this scenario, a state had funded several mobile physician offices in an effort to decrease the costs of providing better health care to disabled elderly in rural areas. Every mobile physician's office had a number of health care monitoring devices that would store PHI about the patients. The office's laptops held updated records for the patients who had appointments, and additional PHI was added to the patients' electronic health care records at the time of each visit. One major omission was physical and logical controls that would protect the security of the PHI the clinicians were collecting during their home visits (e.g., access control, encryption, etc.).

While two clinical staff members were at dinner one evening, their vehicle was stolen. It is unclear whether the thief was only interested in stealing the vehicle or was after the PHI on the laptop and the monitoring devices. This included all forms of PHI such as patient records, patient treatment plans, lab results, doctors' comments, and patient information such as SSNs, drivers license numbers, birth dates, etc.

The patient information was used to perform identity theft and medical identity theft. Several high-profile patients' health care information was made public, leading to embarrassment when personal medical conditions were exposed.

Preventive Measures

Policy:

1. Policies governing the physical and logical controls for mobile staff to properly secure PHI.
2. Policy and governance to equip and train staff performing services outside the health care institution on the specific threats.

Procedures:

1. Implementation of physical security controls to keep patient information secure during transport. Consideration should be given to eliminating all physical patient records from the mobile unit.
2. Implementation of physical security controls to keep patient artifacts (e.g., blood samples) secure during transport.
3. Implementation of strong logical security controls to prevent information from being accessed without proper access credentials.
4. Additional training for personnel who handle the mobile doctor's office.
5. Strong enforcement practices for failing to adhere to the organization's policies.

Technology:

1. Physical security controls for patient records, e.g., lockbox.
2. Encryption with strong key management practices for medical devices, e.g., monitoring, etc.
3. Encryption with strong passwords for mobile computers, e.g., laptops used while in the field.

PHI Threat Scenario #10: Wireless Health Care Device Technology

A hospital staffer brought in non-secure equipment to access Wi-Fi, inadvertently exposing the whole network to an attack using a sniffer.

Wireless technology is a platform of many uses for administrators, clinicians, and support personnel in the health care ecosystem. Wireless technology allows the transmission of 12-lead electrocardiogram (ECG) waveforms from remote locations to handheld computers of cardiologists. Wireless cardiotocography via RF telemetry is being used to monitor the condition of a fetus during labor and has the potential to be adapted for other multi-patient monitoring applications. Wireless terminals are also being used to access medical data during ward rounds. With all the conveniences of wireless health care technology, however, come inherent risks.

At a major hospital in Northern California, in an effort to provide doctors, nurses, and other health care professionals with access to patient information as they moved around their facility, the administration began to connect their clinical information networks with a Wi-Fi network. The medical staff was excited about the opportunity to use their smartphones and tablets to increase their productivity.

Frustrated with the slow progress, and unaware of the hospital's policy for attaching devices to the Wi-Fi network, one staff member brought in an inexpensive consumer grade access point and attached it to the hospital's network. The hospital's network did not have up-to-date DLP technologies or tools to detect rogue access points.

Attackers sitting in a car outside the hospital building gained access to the unprotected network using a sniffer, and several wireless connected health care devices were compromised. Once the attackers gained access through the wireless breach, they were able to access the health care monitoring devices (e.g., Glucose monitor) and steal all forms of PHI, including patient records, patient treatment plans, lab results, doctors' comments, and patients' information such as SSNs, drivers license numbers, birth dates, etc.

Preventive Measures

Policy:

1. All devices must be reviewed and approved by the organization's security team before implementation.

Procedures:

1. Implementation of a strong due-diligence process that provides time-sensitive reviews of new devices so they can be implemented as needed in the health care facility.
2. Strong enforcement practices for failing to adhere to the organization's policies.

Technology:

1. Strong wireless encryption.
2. Rogue wireless detection system.

PHI Threat Scenario #11: State-Sponsored Cyber Crime

Shadowy groups of independent — or state-sponsored — hackers are managing organized attacks on the health care ecosystem. Health care providers often do not have the sophisticated technology required to prevent the attacks, such as intrusion detection tools that trigger early alerts and help to minimize information loss. Health care executives are often unaware of real threats and do not make the necessary investments in security controls.

Attackers seem to have unlimited budgets and time to breach the security protection of health care information. With currently available hacking tools, they gain access to PHI seeking information on the health needs of high-value government officials and use the stolen data for terrorist attacks against them, compromising the government.

The health care provider suffers severe reputational damage as a result of being associated with the terrorist activities. Patient information can be used to perform identity theft and medical identity theft, and is sold on the black market to finance future terrorist activities. Patient records have to be recovered to prevent mistreatments. During the interim time, patient treatments are delayed.

Government agencies must provide additional oversight on health care entities to ensure there are no further breaches.

Preventive Measures

Policy:

1. Strong policies requiring effective network controls.
2. Policy requiring intrusion detection and monitoring.
3. Policy requiring firewalls on all external network connections.

Procedures:

1. Active monitoring of network connections and intrusion detection alerts.
2. Logical separation of network segments.
3. Strong relationships with law enforcement agencies to assist after the detection of an attack.
4. Strong enforcement practices for failing to adhere to the organization's policies.
5. Incident response plan and tests completed on a quarterly basis.

Technology:

1. Network security devices such as firewalls and intelligent switches.
2. Intrusion detection.
3. System log aggregation and intelligent monitoring/review.

APPENDIX E

Complete Results of Survey: Current Practices and Attitudes

A *Survey on Protected Health Information (PHI)* was circulated to the more than 200 PHI project participants and to other subject matter experts responsible for the protection of PHI. The objective of the survey was to determine attitudes, risks, the complexity, the ease of compliance and effects of laws, and the ultimate costs from the loss of PHI data. Participation in the survey was voluntary and the survey was completely anonymous.

The survey responses do not represent a national sampling of the opinions of those responsible for safeguarding PHI, but rather provide some anecdotal insights into the experiences and concerns of PHI protectors.

Of the 131 responses received, 104 respondents were eligible to answer the survey based on their organization's responsibility to collect, use, store, and/or share PHI, or by the association of the organization with a third party who collects, stores, uses, or shares PHI. Not all of the 104 respondents answered all of the questions. Hence, in the data presented below, "n" equals the number of responses received for each question.

Demographics of the Survey Population

Demographic information was obtained on the survey respondents to determine the characteristics of those who were most responsible for safeguarding PHI.

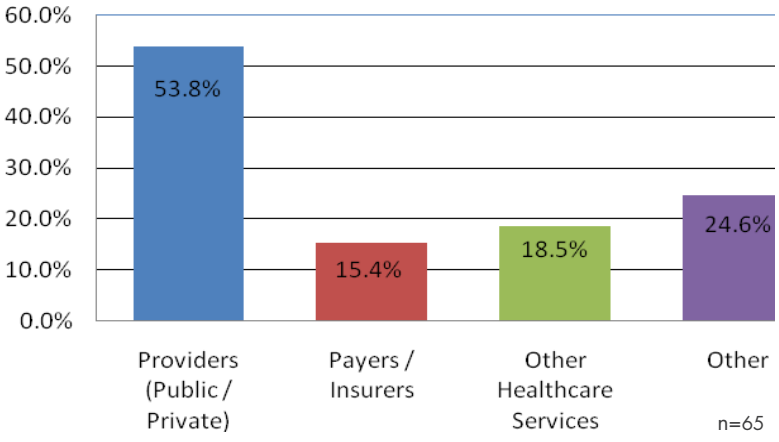


Figure 1 - Participant Role in the Health Care Ecosystem

The survey asked respondents to identify their organization's role in the health care ecosystem (respondents were allowed to choose more than one role). As seen in Figure 1, a majority of respondents (53.8%) identified their organization as a public or private provider of health services. Payers and insurers represented 15.4%, while 18.5% described themselves as other health care service providers and 24.6% described their role as "other." Answers in the "other " category included: home health services; vendor; provider/payer; data recovery of lost information; integrated health systems; assistant services company; two consulting agencies; vendor/business associate; health and wellness education; vendor partner; billing and recovery; provider/insurer/other health services; TAS; business associate; and health care independent software vendor. This question also allowed for multiple responses.

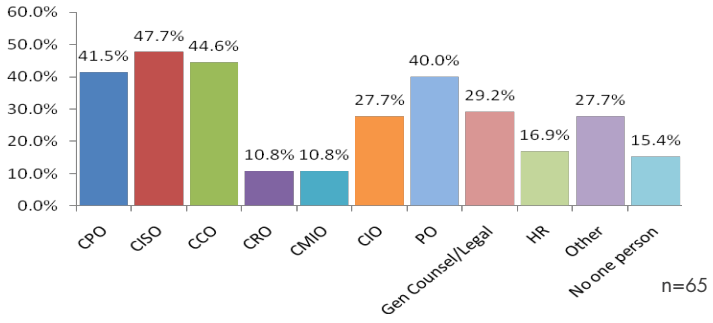


Figure 2 - Overall responsibility for Safeguarding PHI

According to a question regarding who in the organization is responsible for safeguarding PHI (see Figure 2), the majority of the respondents are in the executive level, which includes chief privacy officer, chief information security officer, chief compliance officer, chief risk officer, chief medical information officer, or privacy officer.

Perceived Sensitivity and Effectiveness of Resources to Protect PHI

As indicated in Figure 3, a majority of the respondents (45.5%) utilize a combination of paper and electronic forms of patient records on site. The next highest group (33%) also utilizes a combination of paper and electronic formats, with the organization handling management of records along with the assistance of an outside contractor.

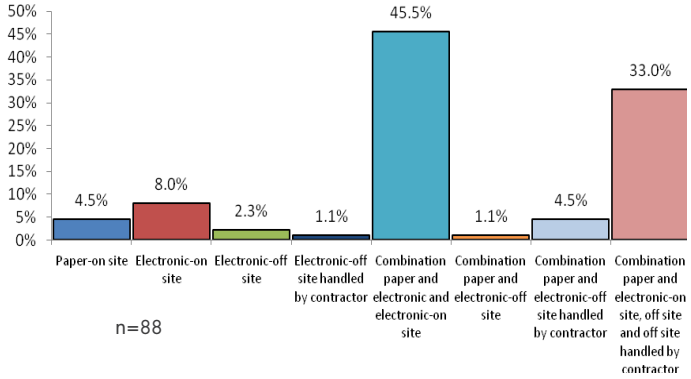


Figure 3 - Type of Records Management by Organization

Survey respondents indicated the number of PHI records their organization is responsible for handling at any one time (see Figure 4). Some 50% of the respondents account for more than 500,000 PHI records with another 43% of the respondents handling 500 to 25,000 records. Respondents ranked the sensitivity of PHI data elements (financial, reputational, medical, or other potential harms) from "low" to "highly sensitive" in the event that data were subject to unauthorized disclosure. The five top data elements identified as highly sensitive by the respondents included:

- Social Security number (97.1%);
- Credit card or bank payment information (95.6%);
- Addictions (87.0%);
- Health history (79.7%); and
- Present illness (76.8%).

Only 47.8% of respondents believe that health insurance identifying information (e.g., policy or identification number), would create a serious impact on their organization if this data were breached. This is a surprising result, since this type of identifying information may be used by another to fraudulently obtain medical service, and may ultimately alter the victim's health records and cause physical harm. The PHI data elements respondents believe to have the least impact include age (14.5%); religion (13%); tied were marital status and educational background (10.3%); also tied were race and ethnicity (10.1%); and, lastly, gender (8.7%).

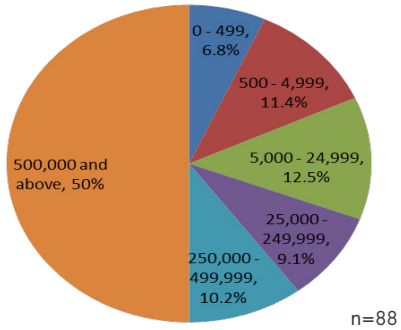


Figure 4 - PHI Survey - Number of PHI Records Responsible for by Organization

A set of key questions sought to elicit perceptions on how effective organizations are in protecting PHI. These included: 1) how strong do respondents believe PHI protection measures are in their organizations; 2) the degree to which senior management prioritizes PHI protection; and 3) whether or not the respondents' organizations were able to devote sufficient resources to PHI protection.

The survey answers indicated that 75% either "strongly agreed" or "agreed" that their organization has implemented effective policies to protect PHI, while 20.8% either "disagreed" or "strongly disagreed" with this statement. The breakdown in responses are similar to the question of whether organizations take "effective steps" to comply with requirements of HIPAA and other related privacy and information security regulations. While 76.4% "agreed" or "strongly agreed" that current actions utilized are effectual, the other 20.8% of respondents "disagreed" or "strongly disagreed" that they are efficient. A question on the perception and attitudes of senior management regarding the prioritizing of privacy and data security yielded a combined 60.6% of those responding either "strongly agreed" or "agreed" that senior management views privacy and data security as a top priority, a combined 28.2% either "disagreed" or "strongly disagreed" with this statement, and 11.3% were "unsure."

Respondents were asked if their organizations possessed sufficient resources to ensure that privacy and data security requirements are currently being met. Of those responding, only 45.8% "strongly agreed" or "agreed" that their organizations had sufficient resources for this, with 31.9% expressing a belief that their organizations did not have sufficient resources to implement protections to safeguard PHI. The remaining 22.2% of the respondents were "unsure" that they had the resources needed to ensure privacy and data security. According to one respondent, "The organization will not fund the necessary tools and staff to maintain compliance."

PHI Security Threats / Protection from Security Threats

Respondents were asked what they perceive to be the most likely current threats affecting their organization's ability to secure PHI. A combined 85.3% stated that the accidental or inadvertent exposure from an insider was the "most likely" or "very likely" threat. Other categories included cyber threats, state-sponsored attacks, malware, malicious insiders, accidental/inadvertent exposure from an insider, social engineering, and inability to prevent loss of media and other devices containing PHI. More than 50% of respondents believe that some type of security threat was likely adversely affecting their organizations now.

Over 80% of the respondents believe that state-sponsored attacks are unlikely to affect their organizations. Another large percentage, 54.4%, believe that it is "very likely" or "likely" that the organization's current threat comes from malicious insiders. Additionally, malware infestation proved to be a great concern for the organizations participating, with 76.1% seeing this as a "very likely" or "likely" threat. A combined 61.2% of respondents feel the organization is "very likely" or "likely" to fall prey to social engineering attacks.

A follow up question asked respondents to indicate whether they believe these threats will worsen within the next three years. Interestingly, the percentage of those who thought state-sponsored attacks would not pose a future threat dropped

to 56.8%. Other areas seen as a greater concern for the future were cyber threats and social engineering. Concerns that accidental or inadvertent exposure from an insider remained high, with 55.1% of survey participants indicating that it is "very likely" or "likely" that future attacks may be perpetrated by malicious insiders. A combined 69.5% of respondents are concerned that security will be compromised by accidental or inadvertent exposure from an insider.

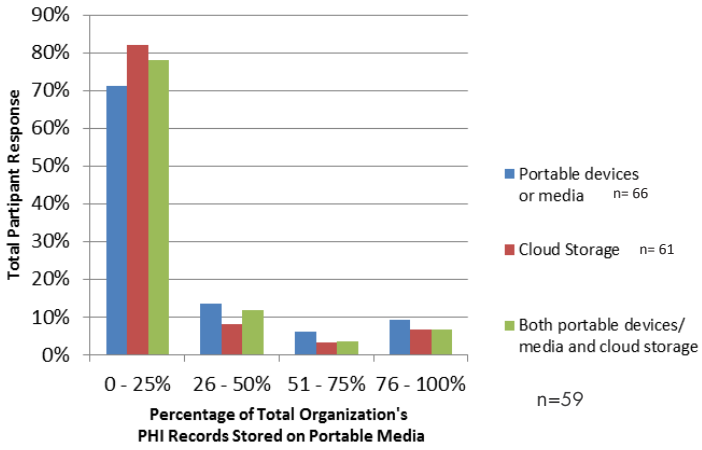


Figure 5 - Percent of Records Managed on Portable Media

The survey also queried respondents regarding the type of portable storage media currently being used by their organization. As indicated in Figure 5, a very small percentage of participants indicated that patient records exist on portable media types such as thumb drives, laptops, CDs, smart phones, or in cloud storage.

The majority of responses, 71.2%, indicated that 0 to 25% of their records reside on portable media devices, while 82% indicated that their records are housed using cloud storage. Additionally, 78% use a combination of cloud storage and portable media devices for 0 to 25% of their records management.

A lesser percentage of survey participants, 19.7%, indicated that 26 to 75% of their organization's records are managed or stored on portable media devices, and 11.5% of records are in cloud storage. A combination of cloud and portable devices are currently being utilized by a total of 15.3% of the participants' organizations. Lastly, a small percentage of survey participants, 9.1%, indicated that 76 to 100% of patient records are housed on portable devices or media, 6.6% utilize cloud storage, and 6.8% use a combination of both platforms.

PHI Breaches and the Financial Impact

The survey asked about both the number of individuals impacted by a data breach by their organization in the last twelve months and the number of breaches estimated. The majority of respondents, 79.4%, stated that less than 500 individuals had been subjected to a data breach; 8.8% of respondents indicated that 500 to 4,999 individuals were impacted; another 5.9% stated that 5,000 to 24,999 individuals were impacted; and 5.9% of respondents stated that 25,000 to 249,999 individuals were affected because of the organization's data breach.

Survey respondents were asked to estimate the number of data breaches involving the exposure, loss, or theft of PHI experienced by their organization during the 12 months prior to the survey. As illustrated in Figure 6, the majority of respondents, a combined 47.7%, stated that their organization's PHI data had been breached in the prior 12 months; 21.5% indicated that they were breached more than 5 times during the same time period; 12.3% had been breached 4 to 5 times; 6.2% of respondents stated that their organization had been breached 2 to 3 times; 7.7% indicated that their organization had been breached only once. Lastly, 6.2% of respondents did not know whether their organization had been affected by any data breach.

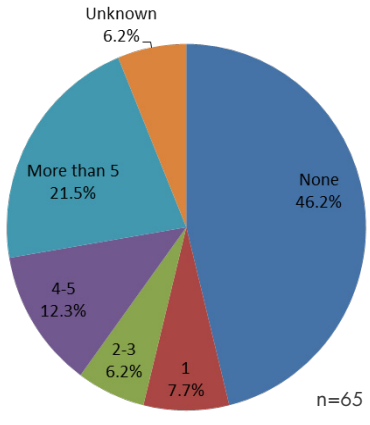


Figure 6 - Number of Breaches Suffered by Organization in Prior 12-Month Period

Respondents also specified whether the individuals affected by the breach were notified by the organization. A combined 50% stated that their organizations notified individuals when all or some data breach incidents were experienced; 31.6% notified individuals only when a significant potential for harm to the individuals' information was forecasted; 5.3% made no data breach notification to individuals; and 13.2% of respondents do not know whether their organization notified individuals when the organization's information was breached.

The number of responses to questions regarding the monetary losses suffered and litigation expenses due to breaches was limited. These respondents indicated that the internal costs associated with the PHI data breach were for expenses related to legal, mitigation, and notification to individuals. In terms of external costs incurred by organizations after experiencing a data breach, seven respondents stated that their organizations' highest expenses were in providing credit or identity monitoring to impacted individuals. Three respondents stated that their organization's external costs were due to computer forensic investigations and legal fees. Only one respondent stated that the organization incurred mitigation expenses.

When asked to estimate the litigation costs suffered by their organizations due to data breach, the majority of respondents who had indicated that their organization had suffered a PHI data breach chose not to respond to this question. The same occurred when questioned to estimate the fines and penalty costs associated with the data breach; only two chose to provide information regarding this. One respondent stated that the costs incurred were for civil monetary penalties. Another respondent stated that the cost incurred was for regulatory fines levied by the Health and Human Services Office for Civil Rights or for violating state laws. It may be that this group of respondents does not know the costs.

When asked to indicate other costs associated with the data breach, five respondents stated that their organizations incurred losses due to reputational harm to the organization, such as loss of goodwill or business loss. Three respondents stated that their organization lost patients. One respondent stated that their organization suffered increased insurance costs. Those nine respondents were queried to approximate the dollar amount of the losses incurred. Five respondents stated that they did not know the amount lost. Four respondents estimated the losses to be $8,000; $100,000; $250,000; and $300,000.

Impediments to Strong Privacy and Data Security

Survey participants identified the most significant obstacles their organizations face to achieve a strong privacy and data security posture with respect to how PHI is collected, used, and retained. This question allowed for multiple answers by respondents. As seen in Figure 7, respondents identified lack of funding (58.5%); insufficient time (40%); nonexistence of senior executive support (32.3%); lack of enabling technologies (27.7%); and the absence of accountability and leadership (27.7%), as the largest concerns to privacy and security. A smaller percentage, 18.5%, stated that there are no significant impediments.

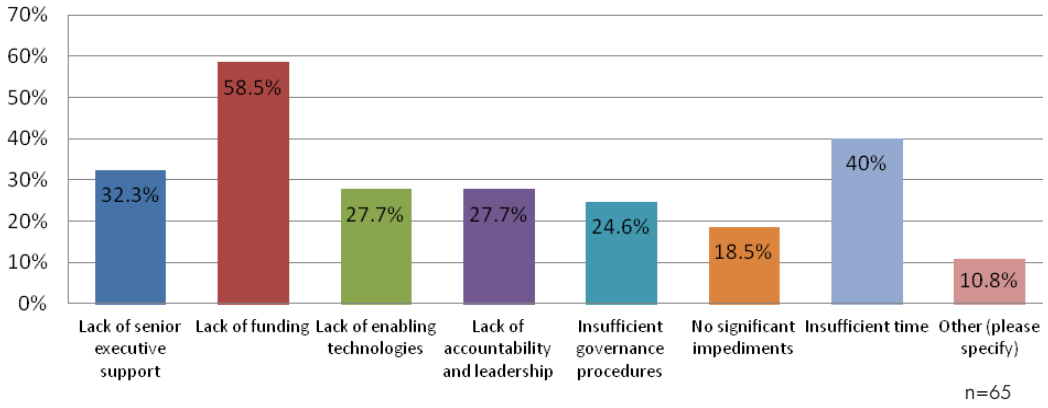


Figure 7 - Most Significant Impediments to Achieving a Strong Privacy and Data Security

Additional comments that respondents provided on impediments that their organizations faced included the following:

- "Complexity of resolving disparate needs and wants of various departments"
- "Getting the bandwidth to highlight privacy and security is so difficult right now when there are so many other conflicting priorities - meaningful use, conversion to new EHR systems, ACOs, Health care reform, quality initiatives, etc."
- "Lack of understanding"
- "Large workforce, varying educational levels, hybrid environment with PHI and ePHI"
- "Need more dedicated personnel"
- "Complexity"
- "User apathy/ignorance"
- "Large organization, lots of turnover, not enough time for training and awareness (too much time spent dealing with issues)"
- "There is so much overlap between laws that analysis is time consuming and difficult"
- "We do not have the employee resources or the funds to deal with additional federal regulations"
- "The laws have been ever changing which makes it difficult to keep pace with policies/procedures and training of employees. The process for passage often is annoying because sometimes facilities are expected to comply with the law before it is 'final.'"
- "OCR tells us that we should not honor state laws that are stricter than HIPAA. They have told us to lobby our state house to change laws. We have spent an inordinate amount of time on this. They tell us we are not reading the law correctly when we say our state law is in conflict with HIPAA."

It appears from the comments of these respondents that there may be insufficient understanding in their organizations of the importance of stressing the legal obligations to protect PHI as well as some lack of understanding of the federal and state regulations. The responses may indicate that implementing standards as prescribed under HITECH and HIPAA, as well as state mandates, may not be given high priority in spending decisions of the organization.

A large majority of respondents could not estimate the cost of complying with HIPAA and HITECH.

Laws: Compliance, Effectiveness, and Complexity

A set of questions was posed to gauge the respondents' knowledge regarding the cost of regulatory compliance and its effectiveness. The first question asked respondents to estimate the cost their organization would incur to comply with HIPAA and HITECH. The majority of respondents (76.6%) did not know the cost. The rest of the respondents estimated the costs to be between $10,000 and over $80 million. The actual amounts given by respondents were: $10,000; 2 responded $15,000; $20,000; $100,000; $250,000; $300,000; $500,000; $1,500,000; $2,000,000; $3,000,000; $50 to $100 million; over $80 million; and millions of dollars. Respondents were asked whether they believed the cost of regulatory compliance would have any effect on the organization's investment in IT initiatives. The majority of respondents (79.4%) believed that their organizations would see an increase in investment in IT initiatives. According to one survey participant, "For large organizations there is usually a large technology price tag that goes to security solutions rather than revenue generating solutions for the company."

Respondents provided their perceptions on the effectiveness of laws currently in place to protect PHI. Results revealed that more than half of the respondents found that some aspect of the law is responsible for a lack of efficacy. The majority of respondents felt that current laws fail in some way to protect information. Some respondents (26.2%) felt that current laws emphasize compliance to the detriment of protecting information. Another 20% believed that current laws fail to achieve adequate protection of information, while 15.4% commented that current laws tend to inhibit treatment of patients in the name of protecting information. According to one survey participant, "They are forcing the cost of health care up! Clinical personnel have to balance good patient care with rules for privacy and security." Only 46.2% of respondents felt that current laws provided effective guidance for protecting information.

When asked how respondents would characterize the complexity of current laws, the majority of respondents (53.8%) found laws to be complex and difficult to understand. Others (35.4%) characterized laws to be overly complex, vague, or confusing. Only 10.8% found current laws easy to understand. Over 56.9% found that maintaining compliance with current laws is somewhat difficult because current laws place some degree of strain on the organization, and 27.7% found it difficult for the organization to maintain compliance with current laws because they place undue stress on the organization. One participant stated, "The laws are difficult to thoroughly understand and require you to view multiple documents to piece it together."

Four main categories arose in quantifying respondents' reasons for perceiving that maintaining compliance with these laws was difficult or somewhat difficult. They were: 1) the conflict between state and federal laws; 2) laws requiring tracking and reporting of everyone who has touched a patient record are unworkable given most current IT systems; 3) scarce financial resources; and 4) technological problems (e.g., systems not set up to achieve full compliance with the regulatory requirements). When asked if compliance with HIPAA and HITECH affects the security of PHI, the vast majority of respondents (79.7%) believed that compliance would increase PHI security.

Summary of What We Learned from the Survey

We undertook the *Survey on Protected Health Information* to discover if participants in the health care industry are investing in the proper decisions to protect PHI, as well as responding properly when a breach of information occurs. This survey also set out to determine what organizations view their risks are presently, and what risks they anticipate will be in their future. The PHI survey also sought information about the obstacles that the responding organizations currently face in order to overcome those risks.

The findings indicated a mix of some possibly surprising and not-so-surprising results for how respondents view the sensitivity of the elements of PHI. Respondents view Social Security numbers and credit card or bank payment information as the most sensitive types of information exposed to a breach. We surmise that this may be because various identity crimes may be committed against the patient if this information is compromised. The results indicated that health insurance identifying information might not be considered as sensitive as other types of information, even though it is typically directly linkable to other PHI data.

Health insurance ID information may not be considered as sensitive as other types of inforamtion, even though it is typically directly linkable to other PHI data.

The survey respondents also indicated that their concerns related to insider threats would drop in the future. This expectation may account in part for the answers received on additional questions that gauged how the participants believed compliance with HIPAA and HITECH would strengthen the security of PHI. Of the 64 who responded, 79.7% stated that compliance would increase the security of PHI. Additionally, 46.2% of the 65 respondents queried about current laws believe that laws in place provide effective guidance for protecting information.

It appears that the greatest concerns are technology, availability of funds, and executive support for funding and manpower to increase security to protect PHI.

There were a limited number of answers regarding the financial costs incurred due to a security breach within the participant organization. When the participants were asked to estimate costs due to a security breach, 78.4% of those who responded did not provide an estimate of the loss. This finding is unclear in its representation. A possible explanation for this result may be that the respondent is not privy to this information due to their position or role within the organization. Alternatively, it could be that the organization did not attempt to calculate the total cost.

A large majority of the participants believed that the cost of mitigating risk and strengthening security was a great impediment. With the complexity and costs to comply, there were anecdotal quotes that indicate that organizations may be facing insufficient time and other constraints to mitigate risk. According to one participant, "We do not have the employee resources or the funds to deal with additional federal regulations." Also, although part of the results indicated that senior management was aware of the great need for security and it was a priority, respondents indicated that they experienced a lack of senior executive support and the absence of accountability and leadership in implementing compliance. One participant stated, "Healthcare information security is behind the times. Senior leaders need to understand legacy protection mechanisms like firewalls are no longer adequate." Those in a risk management role to protect PHI also cited the lack of enabling technologies to safeguard data.

In general, it appears that the greatest concerns are technology, availability of funds, and executive support for funding and manpower to increase security to protect PHI. Complicating this are the various health care privacy laws to which organizations must comply. One participant stated, "Managing medical information across different federal data use and protection regulatory schemes makes it predictable that failures will occur. State and federal laws do not align as well as they could." Additionally, the cost not only affects large organizations, but may be especially burdensome on smaller groups as well. According to one comment from a survey participant, "Being a smaller company, it's difficult to keep up with the costs associated with what is needed." Another stated, "The compliance oriented nature of the healthcare industry makes it more difficult to justify solutions that may better protect information."

Overall, the majority of participants want to comply and secure PHI, but they believe that the lack of executive commitment, leadership and accountability, budgetary constraints, the complexity of compliance with multiple laws, and the evolving nature of the threats and the technologies available to protect PHI combine to make real protection very challenging.

Full-Length Survey Results

The following 36 pages comprise the actual survey results as collected and reported by surveygizmo.com.

Summary Report – Aug 8, 2011
Survey: PHI Project Survey

Note: Pages 9-19 contain crosstabs; individual responses to survey questions start on page 20 with question S1.

Electronic format

Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?

Electronic format	None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
0 – 25%	1 33.3% 3.6%	1 33.3% 33.3%	0 0.0% 0.0%	1 33.3% 12.5%	0 0.0% 0.0%	0 0.0% 0.0%	3 100%
26 – 50%	6 60.0% 21.4%	0 0.0% 0.0%	0 0.0% 0.0%	3 30.0% 37.5%	1 10.0% 7.7%	0 0.0% 0.0%	10 100%
51 – 75%	7 30.4% 25.0%	1 4.3% 33.3%	3 13.0% 75.0%	4 17.4% 50.0%	7 30.4% 53.8%	1 4.3% 33.3%	23 100%
76 – 100%	14 60.9% 50.0%	1 4.3% 33.3%	1 4.3% 25.0%	0 0.0% 0.0%	5 21.7% 38.5%	2 8.7% 66.7%	23 100%
Totals	28 100%	3 100%	4 100%	8 100%	13 100%	3 100%	

Paper form

Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?

Paper form	None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
0 – 25%	16 57.1% 66.7%	1 3.6% 33.3%	1 3.6% 25.0%	3 10.7% 37.5%	6 21.4% 50.0%	1 3.6% 33.3%	28 100%
26 – 50%	3 20.0% 12.5%	1 6.7% 33.3%	1 6.7% 25.0%	3 20.0% 37.5%	6 40.0% 50.0%	1 6.7% 33.3%	15 100%
51 – 75%	2 25.0% 8.3%	1 12.5% 33.3%	2 25.0% 50.0%	2 25.0% 25.0%	0 0.0% 0.0%	1 12.5% 33.3%	8 100%
76 – 100%	3 100.0% 12.5%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	3 100%
Totals	24 100%	3 100%	4 100%	8 100%	12 100%	3 100%	

Both electronic and paper

Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?

Both electronic and paper	None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
0 – 25%	7 46.7% 30.4%	1 6.7% 20.0%	1 6.7% 25.0%	2 13.3% 28.6%	4 26.7% 30.8%	0 0.0% 0.0%	15 100%
26 – 50%	4 57.1% 17.4%	1 14.3% 20.0%	0 0.0% 0.0%	1 14.3% 14.3%	1 14.3% 7.7%	0 0.0% 0.0%	7 100%
51 – 75%	1 12.5% 4.3%	0 0.0% 0.0%	2 25.0% 50.0%	1 12.5% 14.3%	2 25.0% 15.4%	2 25.0% 50.0%	8 100%
76 – 100%	11 42.3% 47.8%	3 11.5% 60.0%	1 3.8% 25.0%	3 11.5% 42.9%	6 23.1% 46.2%	2 7.7% 50.0%	26 100%
	23	5	4	7	13	4	

	Totals	25 100%	3 100%	4 100%	7 100%	13 100%	4 100%

Q13. What was the approximate dollar amount of losses that resulted from data breaches at your organization in the past 12 months?

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
Q13. What was the approximate dollar amount of losses that resulted from data breaches at your organization in the past 12 months?		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
	$	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	4 100.0% 66.7%	0 0.0% 0.0%	4 100%
	Don't know	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	2 40.0% 100.0%	2 40.0% 33.3%	1 20.0% 100.0%	5 100%
	Totals	0 100%	0 100%	0 100%	2 100%	6 100%	1 100%	

Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?

		Q11. Did you attempt to calculate the loss that your organization suffered as a result of data breaches in the past 12 months?		
Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?		Yes	No (Skip to Q14)	Totals
	None (skip to Q14)	0 0.0% 0.0%	2 100.0% 6.9%	2 100%
	1	0 0.0% 0.0%	5 100.0% 17.2%	5 100%
	2 – 3	0 0.0% 0.0%	4 100.0% 13.8%	4 100%
	4 – 5	1 12.5% 12.5%	7 87.5% 24.1%	8 100%
	More than 5	6 42.9% 75.0%	8 57.1% 27.6%	14 100%
	Don't know	1 25.0% 12.5%	3 75.0% 10.3%	4 100%
	Totals	8 100%	29 100%	

D1. What organizational level best describes your current position?

	Q16. How would you characterize the complexity of these laws?			
	Easy to understand	Complex / difficult to understand	Overly complex / vague or confusing	Totals
Senior Executive	0 0.0% 0.0%	5 71.4% 14.3%	2 28.6% 8.7%	7 100%
Vice President	1 20.0% 14.3%	3 60.0% 8.6%	1 20.0% 4.3%	5 100%
Director	0 0.0% 0.0%	11 57.9% 31.4%	8 42.1% 34.8%	19 100%

D1. What organizational level best describes your current position?					
	Manager	1 7.1% 14.3%	8 57.1% 22.9%	5 35.7% 21.7%	14 100%
	Supervisor	0 0.0% 0.0%	1 100.0% 2.9%	0 0.0% 0.0%	1 100%
	Associate/Staff	2 25.0% 28.6%	2 25.0% 5.7%	4 50.0% 17.4%	8 100%
	Technician	0 0.0% 0.0%	1 100.0% 2.9%	0 0.0% 0.0%	1 100%
	Other	3 30.0% 42.9%	4 40.0% 11.4%	3 30.0% 13.0%	10 100%
	Totals	7 100%	35 100%	23 100%	

D1. What organizational level best describes your current position?

		Q17a. How easy is it for your organization to comply with these laws?			
		Not difficult at all — we have all the resources required to maintain compliance within our organization	Somewhat difficult — the current laws place some strain on our organization to maintain compliance	Difficult — the current laws place undue stress on our organization to maintain compliance	Totals
D1. What organizational level best describes your current position?	Senior Executive	2 28.6% 20.0%	4 57.1% 10.8%	1 14.3% 5.6%	7 100%
	Vice President	1 20.0% 10.0%	4 80.0% 10.8%	0 0.0% 0.0%	5 100%
	Director	1 5.3% 10.0%	11 57.9% 29.7%	7 36.8% 38.9%	19 100%
	Manager	2 14.3% 20.0%	7 50.0% 18.9%	5 35.7% 27.8%	14 100%
	Supervisor	0 0.0% 0.0%	1 100.0% 2.7%	0 0.0% 0.0%	1 100%
	Associate/Staff	2 25.0% 20.0%	3 37.5% 8.1%	3 37.5% 16.7%	8 100%
	Technician	1 100.0% 10.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Other	1 10.0% 10.0%	7 70.0% 18.9%	2 20.0% 11.1%	10 100%
	Totals	10 100%	37 100%	18 100%	

D1. What organizational level best describes your current position?

		Q1a. My organization has effective policies and procedures to safeguard PHI.					
		1	2	3	4	5	Totals
D1. What	Senior Executive	3 42.9% 13.6%	1 14.3% 3.7%	0 0.0% 0.0%	2 28.6% 20.0%	1 14.3% 25.0%	7 100%
	Vice President	2 40.0% 9.1%	1 20.0% 3.7%	0 0.0% 0.0%	1 20.0% 10.0%	1 20.0% 25.0%	5 100%
	Director	7 36.8% 31.8%	8 42.1% 29.6%	1 5.3% 50.0%	2 10.5% 20.0%	1 5.3% 25.0%	19 100%
	Manager	5 35.7%	6 42.9%	1 7.1%	2 14.3%	0 0.0%	14 100%

organizational level best describes your current position?	Manager	22.7%	22.2%	50.0%	20.0%	0.0%	
	Supervisor	0 0.0% 0.0%	1 100.0% 3.7%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Associate/Staff	2 25.0% 9.1%	4 50.0% 14.8%	0 0.0% 0.0%	2 25.0% 20.0%	0 0.0% 0.0%	8 100%
	Technician	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 10.0%	0 0.0% 0.0%	1 100%
	Other	3 30.0% 13.6%	6 60.0% 22.2%	0 0.0% 0.0%	0 0.0% 0.0%	1 10.0% 25.0%	10 100%
	Totals	22 100%	27 100%	2 100%	10 100%	4 100%	

D1. What organizational level best describes your current position?

		Q1b. My organization takes effective steps to comply with the requirements of HIPAA and other related privacy and information security regulations.					
		1	2	3	4	5	Totals
D1. What organizational level best describes your current position?	Senior Executive	4 57.1% 16.7%	0 0.0% 0.0%	0 0.0% 0.0%	1 14.3% 12.5%	2 28.6% 33.3%	7 100%
	Vice President	2 40.0% 8.3%	1 20.0% 3.8%	0 0.0% 0.0%	1 20.0% 12.5%	1 20.0% 16.7%	5 100%
	Director	7 36.8% 29.2%	8 42.1% 30.8%	0 0.0% 0.0%	3 15.8% 37.5%	1 5.3% 16.7%	19 100%
	Manager	5 35.7% 20.8%	7 50.0% 26.9%	1 7.1% 100.0%	0 0.0% 0.0%	1 7.1% 16.7%	14 100%
	Supervisor	0 0.0% 0.0%	1 100.0% 3.8%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Associate/Staff	3 37.5% 12.5%	3 37.5% 11.5%	0 0.0% 0.0%	2 25.0% 25.0%	0 0.0% 0.0%	8 100%
	Technician	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 12.5%	0 0.0% 0.0%	1 100%
	Other	3 30.0% 12.5%	6 60.0% 23.1%	0 0.0% 0.0%	0 0.0% 0.0%	1 10.0% 16.7%	10 100%
	Totals	24 100%	26 100%	1 100%	8 100%	6 100%	

D1. What organizational level best describes your current position?

		Q1c. My organization's senior management views privacy and data security as a top priority.					
		1	2	3	4	5	Totals
D1. What organizational level best describes your current	Senior Executive	2 28.6% 10.0%	2 28.6% 11.1%	0 0.0% 0.0%	1 14.3% 10.0%	2 28.6% 22.2%	7 100%
	Vice President	2 40.0% 10.0%	1 20.0% 5.6%	0 0.0% 0.0%	2 40.0% 20.0%	0 0.0% 0.0%	5 100%
	Director	5 26.3% 25.0%	6 31.6% 33.3%	3 15.8% 42.9%	3 15.8% 30.0%	2 10.5% 22.2%	19 100%
	Manager	5 35.7% 25.0%	4 28.6% 22.2%	3 21.4% 42.9%	1 7.1% 10.0%	1 7.1% 11.1%	14 100%
	Supervisor	0 0.0% 0.0%	1 100.0% 5.6%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%

position?	Associate/Staff	1 14.3% 5.0%	3 42.9% 16.7%	1 14.3% 14.3%	1 14.3% 10.0%	1 14.3% 11.1%	7 100%
	Technician	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 10.0%	0 0.0% 0.0%	1 100%
	Other	5 50.0% 25.0%	1 10.0% 5.6%	0 0.0% 0.0%	1 10.0% 10.0%	3 30.0% 33.3%	10 100%
	Totals	20 100%	18 100%	7 100%	10 100%	9 100%	

D1. What organizational level best describes your current position?

		Q1d. My organization has sufficient resources to ensure privacy and data security requirements are met.					
		1	2	3	4	5	Totals
D1. What organizational level best describes your current position?	Senior Executive	2 28.6% 14.3%	2 28.6% 13.3%	1 14.3% 7.1%	1 14.3% 7.1%	1 14.3% 12.5%	7 100%
	Vice President	2 40.0% 14.3%	0 0.0% 0.0%	1 20.0% 7.1%	1 20.0% 7.1%	1 20.0% 12.5%	5 100%
	Director	4 21.1% 28.6%	3 15.8% 20.0%	5 26.3% 35.7%	4 21.1% 28.6%	3 15.8% 37.5%	19 100%
	Manager	3 21.4% 21.4%	4 28.6% 26.7%	2 14.3% 14.3%	4 28.6% 28.6%	1 7.1% 12.5%	14 100%
	Supervisor	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 7.1%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Associate/Staff	2 25.0% 14.3%	2 25.0% 13.3%	2 25.0% 14.3%	1 12.5% 7.1%	1 12.5% 12.5%	8 100%
	Technician	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 7.1%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Other	1 10.0% 7.1%	4 40.0% 26.7%	1 10.0% 7.1%	3 30.0% 21.4%	1 10.0% 12.5%	10 100%
	Totals	14 100%	15 100%	14 100%	14 100%	8 100%	

Q1a. My organization has effective policies and procedures to safeguard PHI.

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Q1a. My organization has effective policies and procedures to safeguard PHI.	1	12 54.5% 40.0%	0 0.0% 0.0%	1 4.5% 25.0%	0 0.0% 0.0%	7 31.8% 50.0%	2 9.1% 50.0%	22 100%
	2	11 40.7% 36.7%	3 11.1% 60.0%	1 3.7% 25.0%	6 22.2% 75.0%	5 18.5% 35.7%	1 3.7% 25.0%	27 100%
	3	1 50.0% 3.3%	0 0.0% 0.0%	1 50.0% 25.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	2 100%
	4	2 20.0% 6.7%	2 20.0% 40.0%	1 10.0% 25.0%	2 20.0% 25.0%	2 20.0% 14.3%	1 10.0% 25.0%	10 100%
	5	4 100.0% 13.3%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	4 100%
	Totals	30 100%	5 100%	4 100%	8 100%	14 100%	4 100%	

Q1b. My organization takes effective steps to comply with the requirements of HIPAA and other related privacy and information security regulations.

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Q1b. My organization takes effective steps to comply with the requirements of HIPAA and other related privacy and information security regulations.	1	12 50.0% 40.0%	1 4.2% 20.0%	1 4.2% 25.0%	2 8.3% 25.0%	6 25.0% 42.9%	2 8.3% 50.0%	24 100%
	2	11 42.3% 36.7%	2 7.7% 40.0%	2 7.7% 50.0%	3 11.5% 37.5%	7 26.9% 50.0%	1 3.8% 25.0%	26 100%
	3	1 100.0% 3.3%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	4	1 12.5% 3.3%	2 25.0% 40.0%	1 12.5% 25.0%	2 25.0% 25.0%	1 12.5% 7.1%	1 12.5% 25.0%	8 100%
	5	5 83.3% 16.7%	0 0.0% 0.0%	0 0.0% 0.0%	1 16.7% 12.5%	0 0.0% 0.0%	0 0.0% 0.0%	6 100%
	Totals	30 100%	5 100%	4 100%	8 100%	14 100%	4 100%	

Q1c. My organization's senior management views privacy and data security as a top priority.

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Q1c. My organization's senior management views privacy and data security as a top priority.	1	12 60.0% 41.4%	1 5.0% 20.0%	1 5.0% 25.0%	0 0.0% 0.0%	4 20.0% 28.6%	2 10.0% 50.0%	20 100%
	2	6 33.3% 20.7%	2 11.1% 40.0%	2 11.1% 50.0%	3 16.7% 37.5%	4 22.2% 28.6%	1 5.6% 25.0%	18 100%
	3	3 42.9% 10.3%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	4 57.1% 28.6%	0 0.0% 0.0%	7 100%
	4	3 30.0% 10.3%	1 10.0% 20.0%	1 10.0% 25.0%	2 20.0% 25.0%	2 20.0% 14.3%	1 10.0% 25.0%	10 100%
	5	5 55.6% 17.2%	1 11.1% 20.0%	0 0.0% 0.0%	3 33.3% 37.5%	0 0.0% 0.0%	0 0.0% 0.0%	9 100%
	Totals	29 100%	5 100%	4 100%	8 100%	14 100%	4 100%	

Q1d. My organization has sufficient resources to ensure privacy and data security requirements are met.

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Q1d. My organization has sufficient resources to ensure privacy and	1	10 71.4% 33.3%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	3 21.4% 21.4%	1 7.1% 25.0%	14 100%
	2	5 33.3% 16.7%	1 6.7% 20.0%	2 13.3% 50.0%	1 6.7% 12.5%	4 26.7% 28.6%	2 13.3% 50.0%	15 100%
	3	6 42.9% 20.0%	2 14.3% 40.0%	1 7.1% 25.0%	1 7.1% 12.5%	3 21.4% 21.4%	1 7.1% 25.0%	14 100%
		5 35.7%	1 7.1%	1 7.1%	4 28.6%	3 21.4%	0 0.0%	14 100%

data security requirements are met.	4	16.7%		20.0%		25.0%		50.0%		21.4%	0.0%	
	5	4 50.0% 13.3%		1 12.5% 20.0%		0 0.0% 0.0%		2 25.0% 25.0%		1 12.5% 7.1%	0 0.0% 0.0%	8 100%
	Totals	30 100%		5 100%		4 100%		8 100%		14 100%	4 100%	

Q10. Approximately, how many individuals were impacted as a result of all data breaches experienced in the past 12 months?

		Q11. Did you attempt to calculate the loss that your organization suffered as a result of data breaches in the past 12 months?		
		Yes	No (Skip to Q14)	Totals
Q10. Approximately, how many individuals were impacted as a result of all data breaches experienced in the past 12 months?	0 – 499 individuals	3 11.5% 42.9%	23 88.5% 88.5%	26 100%
	500 – 4,999 individuals	1 33.3% 14.3%	2 66.7% 7.7%	3 100%
	5,000 – 24,999 individuals	2 100.0% 28.6%	0 0.0% 0.0%	2 100%
	25,000 – 249,999 individuals	1 50.0% 14.3%	1 50.0% 3.8%	2 100%
	250,000 – 499,999 individuals	0 0.0% 0.0%	0 0.0% 0.0%	0 100%
	500,000 and above individuals	0 0.0% 0.0%	0 0.0% 0.0%	0 100%
	Totals	7 100%	26 100%	

Q10. Approximately, how many individuals were impacted as a result of all data breaches experienced in the past 12 months?

		Q13. What was the approximate dollar amount of losses that resulted from data breaches at your organization in the past 12 months?		
		$	Don't know	Totals
Q10. Approximately, how many individuals were impacted as a result of all data breaches experienced in the past 12 months?	0 – 499 individuals	1 25.0% 25.0%	3 75.0% 75.0%	4 100%
	500 – 4,999 individuals	1 100.0% 25.0%	0 0.0% 0.0%	1 100%
	5,000 – 24,999 individuals	2 100.0% 50.0%	0 0.0% 0.0%	2 100%
	25,000 – 249,999 individuals	0 0.0% 0.0%	1 100.0% 25.0%	1 100%
	250,000 – 499,999 individuals	0 0.0% 0.0%	0 0.0% 0.0%	0 100%
	500,000 and above individuals	0 0.0% 0.0%	0 0.0% 0.0%	0 100%
	Totals	4 100%	4 100%	

D7. Which of the following best describes your organization's role in the healthcare ecosystem?

		Q16. How would you characterize the complexity of these laws?			
		Easy to understand	Complex / difficult to understand	Overly complex / vague or confusing	Totals
D7. Which of the following best describes your organization's role in the healthcare ecosystem?	Providers (Public / Private)	5 14.3% 55.6%	17 48.6% 44.7%	13 37.1% 50.0%	35 100%
	Payors / Insurers	1 10.0% 11.1%	7 70.0% 18.4%	2 20.0% 7.7%	10 100%
	Other Healthcare Services	2 16.7% 22.2%	6 50.0% 15.8%	4 33.3% 15.4%	12 100%
	Other (please specify)	1 6.3% 11.1%	8 50.0% 21.1%	7 43.8% 26.9%	16 100%
	Totals	9 100%	38 100%	26 100%	

D7. Which of the following best describes your organization's role in the healthcare ecosystem?

		Q17a. How easy is it for your organization to comply with these laws?			
		Not difficult at all — we have all the resources required to maintain compliance within our organization	Somewhat difficult — the current laws place some strain on our organization to maintain compliance	Difficult — the current laws place undue stress on our organization to maintain compliance	Totals
D7. Which of the following best describes your organization's role in the healthcare ecosystem?	Providers (Public / Private)	5 14.3% 50.0%	18 51.4% 41.9%	12 34.3% 60.0%	35 100%
	Payors / Insurers	1 10.0% 10.0%	8 80.0% 18.6%	1 10.0% 5.0%	10 100%
	Other Healthcare Services	2 16.7% 20.0%	7 58.3% 16.3%	3 25.0% 15.0%	12 100%
	Other (please specify)	2 12.5% 20.0%	10 62.5% 23.3%	4 25.0% 20.0%	16 100%
	Totals	10 100%	43 100%	20 100%	

D1. What organizational level best describes your current position?

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
D1. What organizational level best describes your current position?	Senior Executive	6 85.7% 20.0%	1 14.3% 20.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	7 100%
	Vice President	2 40.0% 6.7%	1 20.0% 20.0%	0 0.0% 0.0%	0 0.0% 0.0%	2 40.0% 14.3%	0 0.0% 0.0%	5 100%
	Director	8 42.1% 26.7%	1 5.3% 20.0%	1 5.3% 25.0%	3 15.8% 37.5%	6 31.6% 42.9%	0 0.0% 0.0%	19 100%
	Manager	7 50.0% 23.3%	0 0.0% 0.0%	0 0.0% 0.0%	2 14.3% 25.0%	5 35.7% 35.7%	0 0.0% 0.0%	14 100%
	Supervisor	1 100.0% 3.3%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Associate/Staff	3 37.5% 10.0%	1 12.5% 20.0%	2 25.0% 50.0%	1 12.5% 12.5%	0 0.0% 0.0%	1 12.5% 25.0%	8 100%
		0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	1 100.0%	1 100%

	Technician	0 0.0% 0.0%		0 0.0% 0.0%		0 0.0% 0.0%		0 0.0% 0.0%		0 0.0% 0.0%		1 100.0% 25.0%	1 100%
	Other	3 30.0% 10.0%		1 10.0% 20.0%		1 10.0% 25.0%		2 20.0% 25.0%		1 10.0% 7.1%		2 20.0% 50.0%	10 100%
	Totals	30 100%		5 100%		4 100%		8 100%		14 100%		4 100%	

D7. Which of the following best describes your organization's role in the healthcare ecosystem?

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
D7. Which of the following best describes your organization's role in the healthcare ecosystem?	Providers (Public / Private)	12 34.3% 35.3%	3 8.6% 60.0%	3 8.6% 75.0%	7 20.0% 70.0%	8 22.9% 50.0%	2 5.7% 50.0%	35 100%
	Payors / Insurers	2 20.0% 5.9%	1 10.0% 20.0%	0 0.0% 0.0%	1 10.0% 10.0%	5 50.0% 31.3%	1 10.0% 25.0%	10 100%
	Other Healthcare Services	8 66.7% 23.5%	0 0.0% 0.0%	1 8.3% 25.0%	1 8.3% 10.0%	2 16.7% 12.5%	0 0.0% 0.0%	12 100%
	Other (please specify)	12 75.0% 35.3%	1 6.3% 20.0%	0 0.0% 0.0%	1 6.3% 10.0%	1 6.3% 6.3%	1 6.3% 25.0%	16 100%
	Totals	34 100%	5 100%	4 100%	10 100%	16 100%	4 100%	

Q20a. Who within your organization is responsible for safeguarding PHI? Please check all that apply.

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Q20a. Who within your organization is responsible for safeguarding PHI? Please check all that apply.	Chief privacy officer	14 51.9% 14.6%	1 3.7% 9.1%	1 3.7% 6.7%	3 11.1% 8.8%	8 29.6% 19.0%	0 0.0% 0.0%	27 100%
	Chief information security officer	15 48.4% 15.6%	2 6.5% 18.2%	1 3.2% 6.7%	4 12.9% 11.8%	9 29.0% 21.4%	0 0.0% 0.0%	31 100%
	Chief compliance officer	11 37.9% 11.5%	2 6.9% 18.2%	3 10.3% 20.0%	4 13.8% 11.8%	7 24.1% 16.7%	2 6.9% 40.0%	29 100%
	Chief risk officer	4 57.1% 4.2%	0 0.0% 0.0%	1 14.3% 6.7%	1 14.3% 2.9%	1 14.3% 2.4%	0 0.0% 0.0%	7 100%
	Chief medical information officer	4 57.1% 4.2%	0 0.0% 0.0%	1 14.3% 6.7%	2 28.6% 5.9%	0 0.0% 0.0%	0 0.0% 0.0%	7 100%
	Chief information officer	9 50.0% 9.4%	0 0.0% 0.0%	1 5.6% 6.7%	5 27.8% 14.7%	3 16.7% 7.1%	0 0.0% 0.0%	18 100%
	Privacy officer	11 42.3% 11.5%	1 3.8% 9.1%	1 3.8% 6.7%	7 26.9% 20.6%	5 19.2% 11.9%	1 3.8% 20.0%	26 100%
	General counsel/legal	10 52.6% 10.4%	1 5.3% 9.1%	1 5.3% 6.7%	4 21.1% 11.8%	3 15.8% 7.1%	0 0.0% 0.0%	19 100%
	Human resources	6 54.5% 6.3%	1 9.1% 9.1%	2 18.2% 13.3%	1 9.1% 2.9%	1 9.1% 2.4%	0 0.0% 0.0%	11 100%
	Other (please specify)	6 33.3% 6.3%	2 11.1% 18.2%	1 5.6% 6.7%	3 16.7% 8.8%	5 27.8% 11.9%	1 5.6% 20.0%	18 100%
	No one person has overall responsibility	6 60.0% 6.3%	1 10.0% 9.1%	2 20.0% 13.3%	0 0.0% 0.0%	0 0.0% 0.0%	1 10.0% 20.0%	10 100%

	Unsure	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 100%
	Totals	96 100%	11 100%	15 100%	34 100%	42 100%	5 100%	

Q20b. Which of these individuals is most responsible for safeguarding PHI?

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Q20b. Which of these individuals is most responsible for safeguarding PHI?	Chief privacy officer	8 42.1% 21.1%	1 5.3% 16.7%	1 5.3% 14.3%	1 5.3% 10.0%	7 36.8% 41.2%	1 5.3% 12.5%	19 100%
	Chief information security officer	10 55.6% 26.3%	1 5.6% 16.7%	1 5.6% 14.3%	3 16.7% 30.0%	3 16.7% 17.6%	0 0.0% 0.0%	18 100%
	Chief compliance officer	5 50.0% 13.2%	0 0.0% 0.0%	3 30.0% 42.9%	0 0.0% 0.0%	1 10.0% 5.9%	1 10.0% 12.5%	10 100%
	Chief risk officer	0 0.0% 0.0%	1 50.0% 16.7%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 50.0% 12.5%	2 100%
	Chief medical information officer	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 100%
	Chief information officer	3 75.0% 7.9%	0 0.0% 0.0%	0 0.0% 0.0%	1 25.0% 10.0%	0 0.0% 0.0%	0 0.0% 0.0%	4 100%
	Privacy officer	6 35.3% 15.8%	1 5.9% 16.7%	1 5.9% 14.3%	3 17.6% 30.0%	4 23.5% 23.5%	2 11.8% 25.0%	17 100%
	General counsel/legal	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 12.5%	1 100%
	Human resources	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 12.5%	1 100%
	Other (please specify)	2 25.0% 5.3%	1 12.5% 16.7%	1 12.5% 14.3%	2 25.0% 20.0%	2 25.0% 11.8%	0 0.0% 0.0%	8 100%
	No one person has overall responsibility	4 66.7% 10.5%	1 16.7% 16.7%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 16.7% 12.5%	6 100%
	Unsure	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 100%
	Totals	38 100%	6 100%	7 100%	10 100%	17 100%	8 100%	

Q7a. What is your organization doing today to safeguard PHI (both electronic and paper)? Please check all that apply.

		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
	Training and awareness programs for everyone who has access to PHI	30 47.6% 7.2%	5 7.9% 7.0%	3 4.8% 6.4%	7 11.1% 6.7%	14 22.2% 6.8%	4 6.3% 8.9%	63 100%
	Policies and procedures including an incident response plan	28 48.3% 6.7%	5 8.6% 7.0%	3 5.2% 6.4%	6 10.3% 5.8%	13 22.4% 6.3%	3 5.2% 6.7%	58 100%
	VPN, gateway or other network security controls	28 45.2% 6.7%	5 8.1% 7.0%	4 6.5% 8.5%	8 12.9% 7.7%	14 22.6% 6.8%	3 4.8% 6.7%	62 100%

Q7a. What is your organization doing today to safeguard PHI (both electronic and paper)? Please check all that apply.	Encryption for data at rest	21 48.8% 5.1%	4 9.3% 5.6%	3 7.0% 6.4%	5 11.6% 4.8%	9 20.9% 4.4%	1 2.3% 2.2%	43 100%
	Encryption for data in motion	23 46.9% 5.5%	4 8.2% 5.6%	3 6.1% 6.4%	6 12.2% 5.8%	11 22.4% 5.3%	2 4.1% 4.4%	49 100%
	Perimeter controls such as multilayered firewalls	26 44.8% 6.3%	4 6.9% 5.6%	4 6.9% 8.5%	7 12.1% 6.7%	14 24.1% 6.8%	3 5.2% 6.7%	58 100%
	Security guards	16 38.1% 3.9%	4 9.5% 5.6%	2 4.8% 4.3%	5 11.9% 4.8%	12 28.6% 5.8%	3 7.1% 6.7%	42 100%
	Video security system	16 41.0% 3.9%	3 7.7% 4.2%	3 7.7% 6.4%	5 12.8% 4.8%	10 25.6% 4.9%	2 5.1% 4.4%	39 100%
	Data loss prevention tools	17 45.9% 4.1%	4 10.8% 5.6%	1 2.7% 2.1%	4 10.8% 3.8%	9 24.3% 4.4%	2 5.4% 4.4%	37 100%
	Intrusion detection systems	24 50.0% 5.8%	3 6.3% 4.2%	1 2.1% 2.1%	5 10.4% 4.8%	13 27.1% 6.3%	2 4.2% 4.4%	48 100%
	Data retention systems and practices	24 48.0% 5.8%	5 10.0% 7.0%	2 4.0% 4.3%	5 10.0% 4.8%	11 22.0% 5.3%	3 6.0% 6.7%	50 100%
	Anti-virus, anti-malware systems	29 47.5% 7.0%	5 8.2% 7.0%	3 4.9% 6.4%	7 11.5% 6.7%	14 23.0% 6.8%	3 4.9% 6.7%	61 100%
	Correlation and event management systems	13 52.0% 3.1%	1 4.0% 1.4%	1 4.0% 2.1%	2 8.0% 1.9%	7 28.0% 3.4%	1 4.0% 2.2%	25 100%
	Database scanning solutions	15 51.7% 3.6%	2 6.9% 2.8%	1 3.4% 2.1%	3 10.3% 2.9%	7 24.1% 3.4%	1 3.4% 2.2%	29 100%
	Identity and access management solutions	22 46.8% 5.3%	5 10.6% 7.0%	3 6.4% 6.4%	5 10.6% 4.8%	10 21.3% 4.9%	2 4.3% 4.4%	47 100%
	Audit logs	26 47.3% 6.3%	4 7.3% 5.6%	3 5.5% 6.4%	7 12.7% 6.7%	12 21.8% 5.8%	3 5.5% 6.7%	55 100%
	Multifactor authentication	19 51.4% 4.6%	2 5.4% 2.8%	3 8.1% 6.4%	3 8.1% 2.9%	8 21.6% 3.9%	2 5.4% 4.4%	37 100%
	Controlled physical access (including lockable doors, drawers and filing cabinets)	26 43.3% 6.3%	5 8.3% 7.0%	4 6.7% 8.5%	8 13.3% 7.7%	14 23.3% 6.8%	3 5.0% 6.7%	60 100%
	Mobile security management suite	11 45.8% 2.7%	1 4.2% 1.4%	0 0.0% 0.0%	6 25.0% 5.8%	4 16.7% 1.9%	2 8.3% 4.4%	24 100%
	Other (please specify)	1 100.0% 0.2%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Totals	415 100%	71 100%	47 100%	104 100%	206 100%	45 100%	

D1. What organizational level best describes your current position?

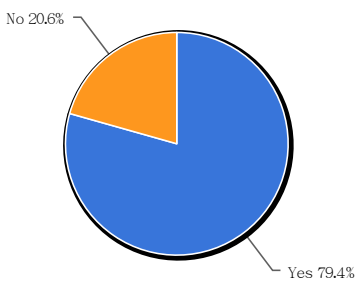
		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
D1. What organizational	Senior Executive	6 85.7% 20.0%	1 14.3% 20.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	7 100%
	Vice President	2 40.0% 6.7%	1 20.0% 20.0%	0 0.0% 0.0%	0 0.0% 0.0%	2 40.0% 14.3%	0 0.0% 0.0%	5 100%
	Director	8 42.1% 26.7%	1 5.3% 20.0%	1 5.3% 25.0%	3 15.8% 37.5%	6 31.6% 42.9%	0 0.0% 0.0%	19 100%
	Manager	7 50.0% 23.3%	0 0.0% 0.0%	0 0.0% 0.0%	2 14.3% 25.0%	5 35.7% 35.7%	0 0.0% 0.0%	14 100%

level best describes your current position?	Supervisor	1 100.0% 3.3%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100%
	Associate/Staff	3 37.5% 10.0%	1 12.5% 20.0%	2 25.0% 50.0%	1 12.5% 12.5%	0 0.0% 0.0%	1 12.5% 25.0%	8 100%
	Technician	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 25.0%	1 100%
	Other	3 30.0% 10.0%	1 10.0% 20.0%	1 10.0% 25.0%	2 20.0% 25.0%	1 10.0% 7.1%	2 20.0% 50.0%	10 100%
	Totals	30 100%	5 100%	4 100%	8 100%	14 100%	4 100%	

D1. What organizational level best describes your current position?

		Q20b. Which of these individuals is most responsible for safegua								
		Chief privacy officer	Chief information security officer	Chief compliance officer	Chief risk officer	Chief medical information officer	Chief information officer	Privacy officer	General counsel/legal	Huma resour
D1. What organizational level best describes your current position?	Senior Executive	2 20.0% 10.5%	2 20.0% 11.1%	1 10.0% 10.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 10.0% 25.0%	1 10.0% 5.9%	0 0.0% 0.0%	0 0.0%
	Vice President	3 50.0% 15.8%	2 33.3% 11.1%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 16.7% 25.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0%
	Director	6 24.0% 31.6%	9 36.0% 50.0%	3 12.0% 30.0%	1 4.0% 50.0%	0 0.0% 0.0%	1 4.0% 25.0%	4 16.0% 23.5%	0 0.0% 0.0%	0 0.0%
	Manager	4 25.0% 21.1%	2 12.5% 11.1%	2 12.5% 20.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 6.3% 25.0%	5 31.3% 29.4%	0 0.0% 0.0%	0 0.0%
	Supervisor	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 5.9%	0 0.0% 0.0%	0 0.0%
	Associate/Staff	3 27.3% 15.8%	2 18.2% 11.1%	1 9.1% 10.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 9.1% 5.9%	0 0.0% 0.0%	0 0.0%
	Technician	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	1 100.0% 5.9%	0 0.0% 0.0%	0 0.0%
	Other	1 6.3% 5.3%	1 6.3% 5.6%	3 18.8% 30.0%	1 6.3% 50.0%	0 0.0% 0.0%	0 0.0% 0.0%	4 25.0% 23.5%	1 6.3% 100.0%	1 6 100.0%
	Totals	19 100%	18 100%	10 100%	2 100%	0 100%	4 100%	17 100%	1 100%	1 100%

S1. Is your organization responsible for the collection, use, storage, or sharing of PHI, or does your organization contract with a third party to collect, store, use or share PHI?

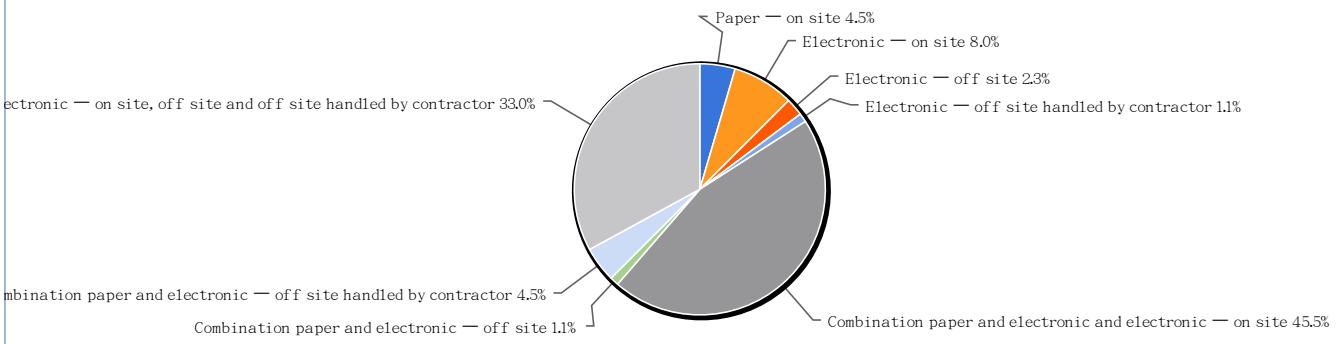


S1. Is your organization responsible for the collection, use, storage, or sharing of PHI, or does your organization contract with a third party to collect, store, use or share PHI?

Value	Count	Percent %
Yes	104	79.4%
No	27	20.6%

Statistics	
Total Responses	131

S2. Which of the below PHI records management descriptions best describes your organization (select one)?

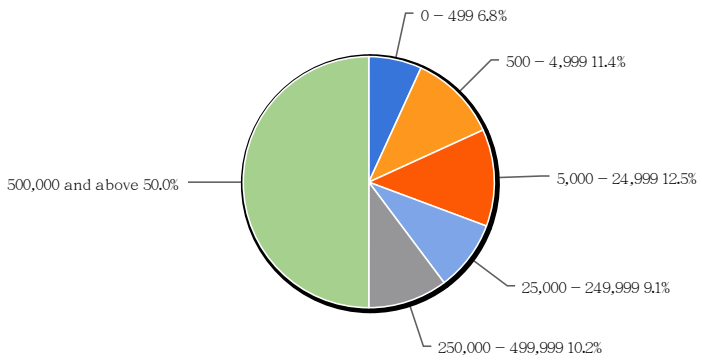


S2. Which of the below PHI records management descriptions best describes your organization (select one)?

Value	Count	Percent %
Paper — on site	4	4.5%
Electronic — on site	7	8%
Electronic — off site	2	2.3%
Electronic — off site handled by contractor	1	1.1%
Combination paper and electronic and electronic — on site	40	45.5%
Combination paper and electronic — off site	1	1.1%
Combination paper and electronic — off site handled by contractor	4	4.5%
Combination paper and electronic — on site, off site and off site handled by contractor	29	33%

Statistics	
Total Responses	88

S3. Number of PHI records that your organization is responsible for at any one time:



S3. Number of PHI records that your organization is responsible for at any one time:

Value	Count	Percent %
0 – 499	6	6.8%
500 – 4,999	10	11.4%
5,000 – 24,999	11	12.5%

Statistics	
Total Responses	88
Sum	29,505.0

25,000 – 249,999	8	9.1%
250,000 – 499,999	9	10.2%
500,000 and above	44	50%

Average	359.8
StdDev	205.16
Max	500.0

Q1. Please respond to each statement using this five-point scale to express your opinion. 1=Strongly agree, 2=Agree, 3=Unsure, 4=Disagree, 5=Strongly disagree

	1	2	3	4	5	Totals
Q1a. My organization has effective policies and procedures to safeguard PHI.	26 36.1%	28 38.9%	3 4.2%	10 13.9%	5 6.9%	72 100%
Q1b. My organization takes effective steps to comply with the requirements of HIPAA and other related privacy and information security regulations.	29 40.3%	26 36.1%	2 2.8%	8 11.1%	7 9.7%	72 100%
Q1c. My organization's senior management views privacy and data security as a top priority.	23 32.4%	20 28.2%	8 11.3%	10 14.1%	10 14.1%	71 100%
Q1d. My organization has sufficient resources to ensure privacy and data security requirements are met.	16 22.2%	17 23.6%	16 22.2%	14 19.4%	9 12.5%	72 100%

Q2. For each of the PHI data elements listed below, please indicate the level of impact (financial, reputation, medical, or other potential harms) if it were subject to an unauthorized disclosure. 1 = Low or no moderate, 2 = Somewhat sensitive 3= Moderately sensitive, 4 = Highly sensitive

	1	2	3	4	Totals
Name	22 31.9%	9 13.0%	16 23.2%	22 31.9%	69 100%
Address	16 23.2%	19 27.5%	19 27.5%	15 21.7%	69 100%
Telephone number	15 21.7%	23 33.3%	15 21.7%	16 23.2%	69 100%
Age	17 24.6%	24 34.8%	18 26.1%	10 14.5%	69 100%
Date of Birth	5 7.2%	12 17.4%	23 33.3%	29 42.0%	69 100%
Gender	31 44.9%	21 30.4%	11 15.9%	6 8.7%	69 100%
Race	27 39.1%	26 37.7%	9 13.0%	7 10.1%	69 100%
Religion	29 42.0%	18 26.1%	13 18.8%	9 13.0%	69 100%
Ethnicity	31 44.9%	19 27.5%	12 17.4%	7 10.1%	69 100%
Sexual preference	8 11.8%	10 14.7%	18 26.5%	32 47.1%	68 100%
Physical characteristics such as weight, height	9 13.0%	30 43.5%	17 24.6%	13 18.8%	69 100%
Family health history	1 1.4%	13 18.8%	20 29.0%	35 50.7%	69 100%
Guardian or emergency contact	11 15.9%	21 30.4%	23 33.3%	14 20.3%	69 100%
Health history	0 0.0%	3 4.3%	11 15.9%	55 79.7%	69 100%
Present illnesses	0 0.0%	3 4.3%	13 18.8%	53 76.8%	69 100%

Photo, x-ray or MRI	1 1.4%	6 8.7%	20 29.0%	42 60.9%	69 100%
Medications	0 0.0%	2 2.9%	15 21.7%	52 75.4%	69 100%
Surgeries	1 1.4%	5 7.2%	16 23.2%	47 68.1%	69 100%
Diet & exercise habits or behavior	3 4.3%	18 26.1%	25 36.2%	23 33.3%	69 100%
Addictions	1 1.4%	1 1.4%	7 10.1%	60 87.0%	69 100%
Employer	16 23.5%	15 22.1%	22 32.4%	15 22.1%	68 100%
Marital status	20 29.4%	26 38.2%	15 22.1%	7 10.3%	68 100%
Participation in clinical trials	5 7.4%	12 17.6%	16 23.5%	35 51.5%	68 100%
Names of health care providers	6 8.7%	16 23.2%	24 34.8%	23 33.3%	69 100%
Social Security number	1 1.4%	0 0.0%	1 1.4%	67 97.1%	69 100%
Internal medical record/account number	3 4.3%	17 24.6%	18 26.1%	31 44.9%	69 100%
Health insurance information	2 2.9%	9 13.0%	25 36.2%	33 47.8%	69 100%
Educational background	26 38.2%	24 35.3%	11 16.2%	7 10.3%	68 100%
Credit card or bank payment information	2 2.9%	0 0.0%	1 1.5%	65 95.6%	68 100%
Credit or payment history	1 1.4%	6 8.7%	10 14.5%	52 75.4%	69 100%

Q3. Please describe the percentage of PHI records managed by your organization that is stored in each format.

	0 - 25%	26 - 50%	51 - 75%	76 - 100%	Totals
Electronic format	4 6.6%	11 18.0%	23 37.7%	23 37.7%	61 100%
Paper form	28 50.0%	16 28.6%	9 16.1%	3 5.4%	56 100%
Both electronic and paper	15 25.0%	7 11.7%	9 15.0%	29 48.3%	60 100%

Q4. What percentage of the EPHI records managed by your organization resides on portable devices or media (i.e., laptops, thumb drives, CDs, smart phones, etc.) or in the cloud?

	0 - 25%	26 - 50%	51 - 75%	76 - 100%	Totals
Portable devices or media	47 71.2%	9 13.6%	4 6.1%	6 9.1%	66 100%
Cloud Storage	50 82.0%	5 8.2%	2 3.3%	4 6.6%	61 100%
Both portable devices/media and cloud storage	46 78.0%	7 11.9%	2 3.4%	4 6.8%	59 100%

Q5. To indicate the risk that database applications present to your organization's EPHI, please order the following application categories from 5 = most at risk to 1 = least at risk for a data breach

Item	Total Score[1]	Overall Rank
Applications used in sales and marketing such as customer relationship management (CRM) systems	225	1
Applications used for governance / oversight / root cause analysis purposes such as investigations; litigation holds … typically data in this category replicates data held elsewhere but does include 'new' information.	208	2
Applications used in treatment such as ADT (admit, discharge & transfer): this includes demographic, plan information but feeds other systems); MARS (medication administration record system); CPOE (order entry); PACS (imaging); labs; biomedical (monitoring systems)	137	3
Applications used in documentation such as electronic record systems; dictation / transcription systems, applications used for a variety of 'governance' purposes such as utilization reviews, accreditation, etc.	122	4
Applications used in reimbursement such as patient accounting systems; billing systems	122	5

Total Respondents: 65

[1] Score is a weighted calculation. Items ranked first are valued higher than the following ranks, the score is the sum of all weighted rank counts.

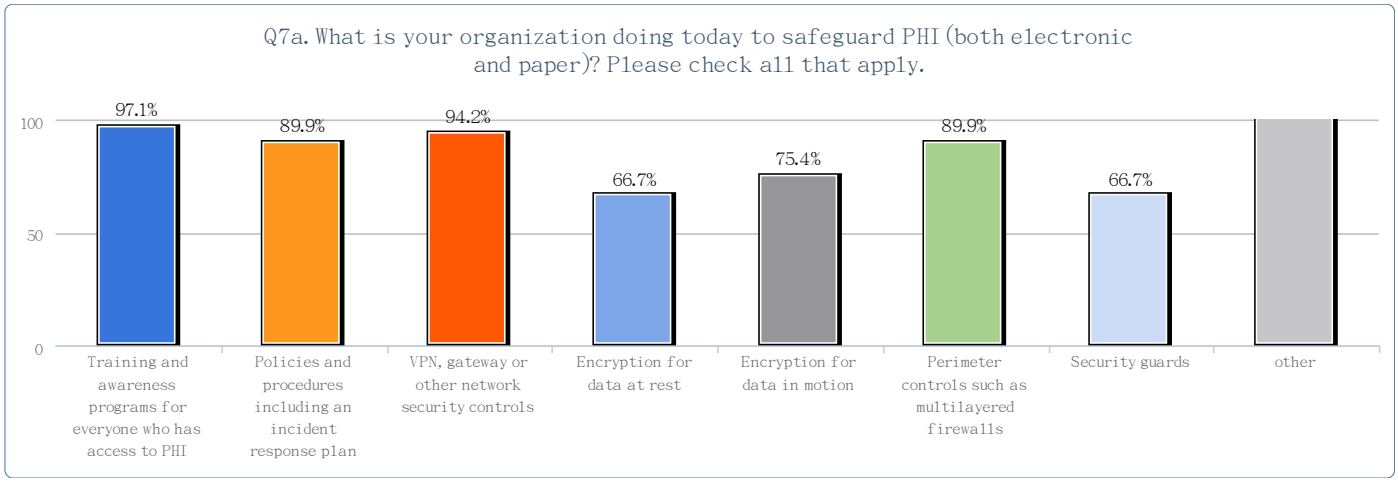
Q6a. What do you see as the mostly likely current threats that may affect your organization's ability to secure PHI?

	Very likely	Likely	Not likely	Not applicable	Totals
Cyber threats	16 23.9%	27 40.3%	23 34.3%	1 1.5%	67 100%
State-sponsored attacks	5 7.7%	5 7.7%	51 78.5%	4 6.2%	65 100%
Malware	21 31.3%	30 44.8%	15 22.4%	1 1.5%	67 100%
Malicious insiders	16 23.5%	21 30.9%	29 42.6%	2 2.9%	68 100%
Accidental or inadvertent exposure from an insider	30 44.1%	28 41.2%	9 13.2%	1 1.5%	68 100%
Social engineering	15 22.4%	26 38.8%	22 32.8%	4 6.0%	67 100%
Inability to prevent loss of media and other devices containing PHI	17 25.0%	22 32.4%	27 39.7%	2 2.9%	68 100%

Q6b. Looking at the same threats, please indicate if you believe they are likely to worsen in the next year to three years.

	Very likely	Likely	Not likely	Not applicable	Totals
Cyber threats	37 53.6%	23 33.3%	8 11.6%	1 1.4%	69 100%
State-sponsored attacks	12 17.9%	17 25.4%	32 47.8%	6 9.0%	67 100%
Malware	36 53.7%	19 28.4%	11 16.4%	1 1.5%	67 100%
Malicious insiders	18 26.1%	20 29.0%	30 43.5%	1 1.4%	69 100%
Accidental or inadvertent exposure from an insider	25 36.2%	23 33.3%	20 29.0%	1 1.4%	69 100%
Social engineering	17 24.6%	34 49.3%	15 21.7%	3 4.3%	69 100%

Social engineering	14	20.3%	34	49.3%	18	26.1%	3	4.3%	69	100%
Inability to prevent loss of media and other devices containing PHI	21	30.4%	20	29.0%	26	37.7%	2	2.9%	69	100%

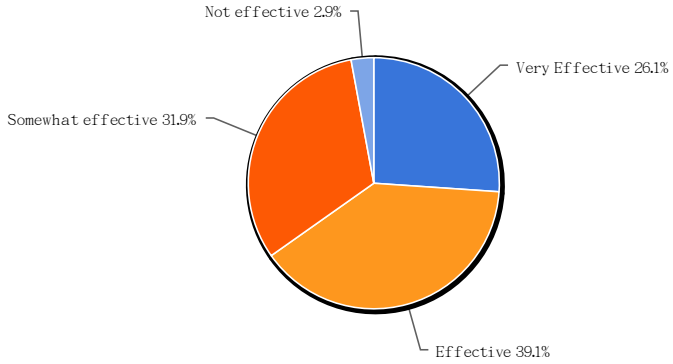


Q7a. What is your organization doing today to safeguard PHI (both electronic and paper)? Please check all that apply.

Value	Count	Percent %
Training and awareness programs for everyone who has access to PHI	67	97.1%
Policies and procedures including an incident response plan	62	89.9%
VPN, gateway or other network security controls	65	94.2%
Encryption for data at rest	46	66.7%
Encryption for data in motion	52	75.4%
Perimeter controls such as multilayered firewalls	62	89.9%
Security guards	46	66.7%
Video security system	43	62.3%
Data loss prevention tools	38	55.1%
Intrusion detection systems	52	75.4%
Data retention systems and practices	53	76.8%
Anti-virus, anti-malware systems	65	94.2%
Correlation and event management systems	26	37.7%
Database scanning solutions	31	44.9%
Identity and access management solutions	51	73.9%
Audit logs	59	85.5%
Multifactor authentication	40	58%
Controlled physical access (including lockable doors, drawers and filing cabinets)	64	92.8%
Mobile security management suite	25	36.2%
Other (please specify)	1	1.4%

Statistics	
Total Responses	69

Q7b. How would you rate the effectiveness of the above mentioned data security measures you have in-place for securing PHI?

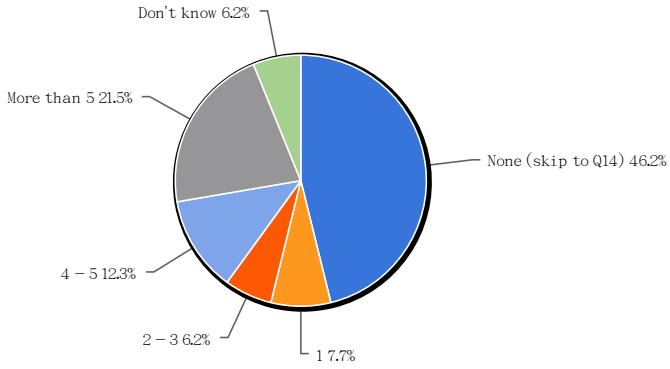


Q7b. How would you rate the effectiveness of the above mentioned data security measures you have in-place for securing PHI?

Value	Count	Percent %
Very Effective	18	26.1%
Effective	27	39.1%
Somewhat effective	22	31.9%
Not effective	2	2.9%

Statistics	
Total Responses	69

Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?

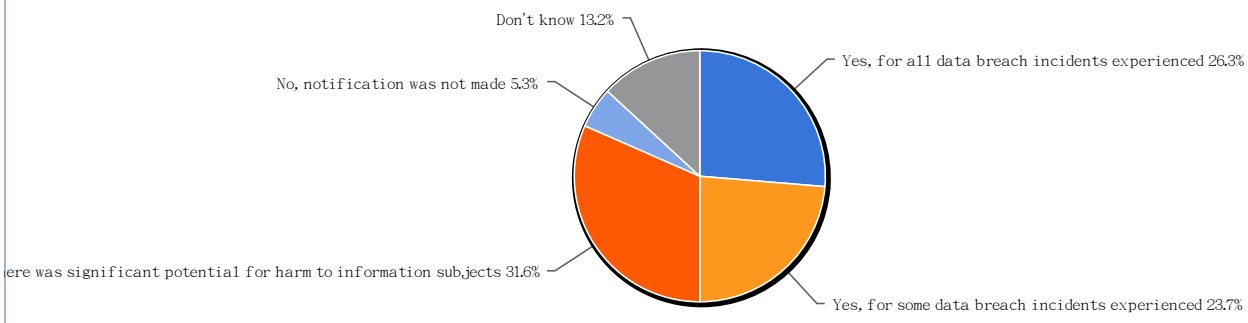


Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?

Value	Count	Percent %
None (skip to Q14)	30	46.2%
1	5	7.7%
2 - 3	4	6.2%
4 - 5	8	12.3%
More than 5	14	21.5%
Don't know	4	6.2%

Statistics	
Total Responses	65
Sum	45.0
Average	2.6
StdDev	1.33
Max	4.0

Q9. Did your organization notify individuals whose information was breached in the past 12 months?

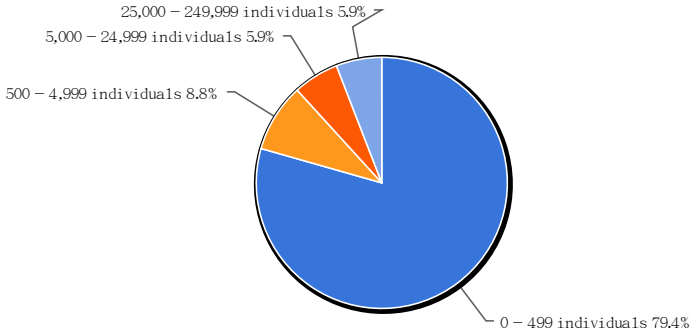


Q9. Did your organization notify individuals whose information was breached in the past 12 months?

Value	Count	Percent %
Yes, for all data breach incidents experienced	10	26.3%
Yes, for some data breach incidents experienced	9	23.7%
Yes, for some data breach incidents experienced where there was significant potential for harm to information subjects	12	31.6%
No, notification was not made	2	5.3%
Don't know	5	13.2%

Statistics	
Total Responses	38

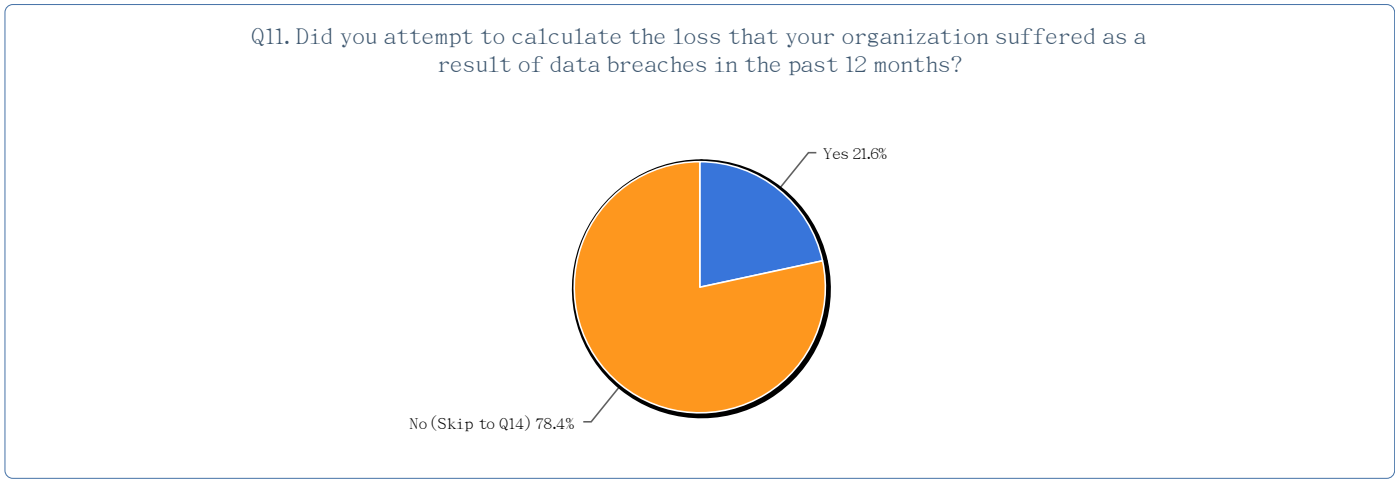
Q10. Approximately, how many individuals were impacted as a result of all data breaches experienced in the past 12 months?



Q10. Approximately, how many individuals were impacted as a result of all data breaches experienced in the past 12 months?

Value	Count	Percent %
0 – 499 individuals	27	79.4%
500 – 4,999 individuals	3	8.8%
5,000 – 24,999 individuals	2	5.9%
25,000 – 249,999 individuals	2	5.9%

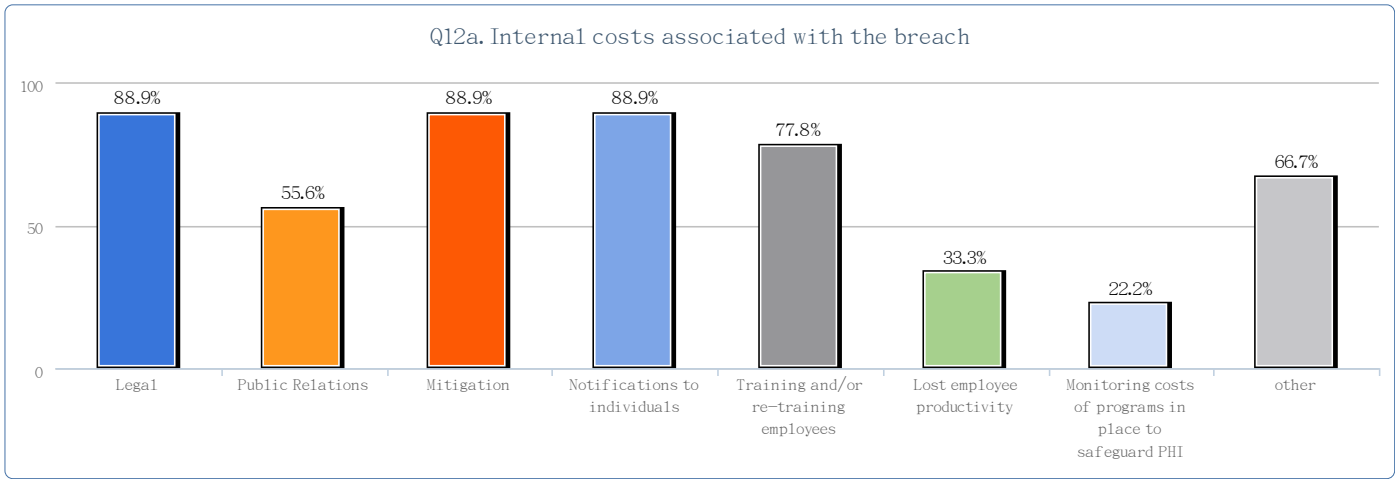
Statistics	
Total Responses	34
Sum	1,560.0
Average	222.9
StdDev	240.13
Max	500.0



Q11. Did you attempt to calculate the loss that your organization suffered as a result of data breaches in the past 12 months?

Value	Count	Percent %
Yes	8	21.6%
No (Skip to Q14)	29	78.4%

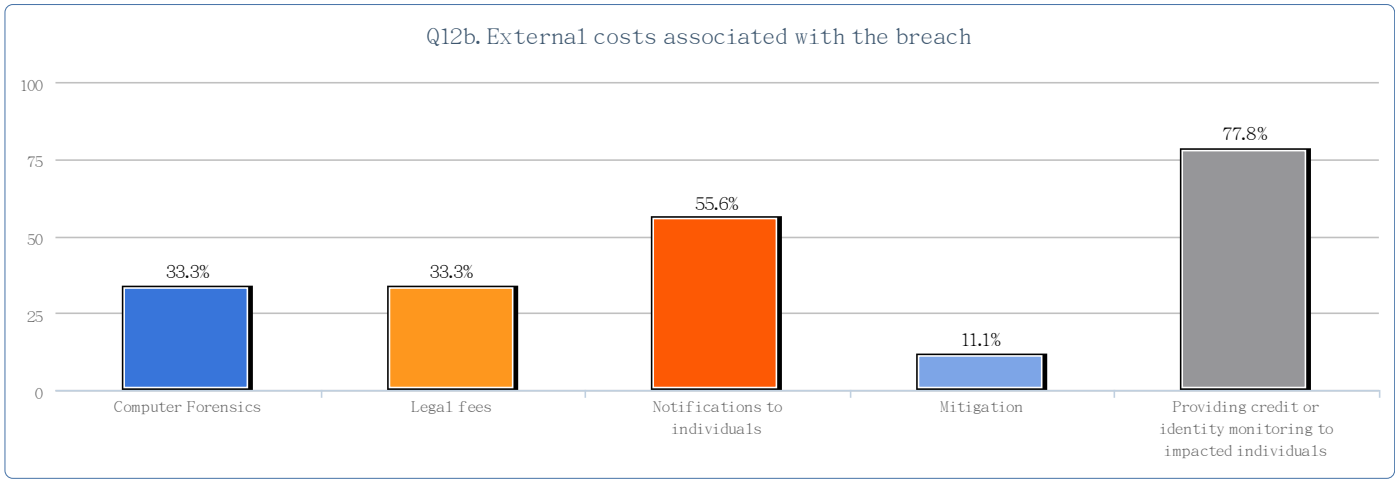
Statistics	
Total Responses	37



Q12a. Internal costs associated with the breach

Value	Count	Percent %
Legal	8	88.9%
Public Relations	5	55.6%
Mitigation	8	88.9%
Notifications to individuals	8	88.9%
Training and/or re-training employees	7	77.8%
Lost employee productivity	3	33.3%
Monitoring costs of programs in place to safeguard PHI	2	22.2%
Computer Forensics and other internal investigating costs	6	66.7%

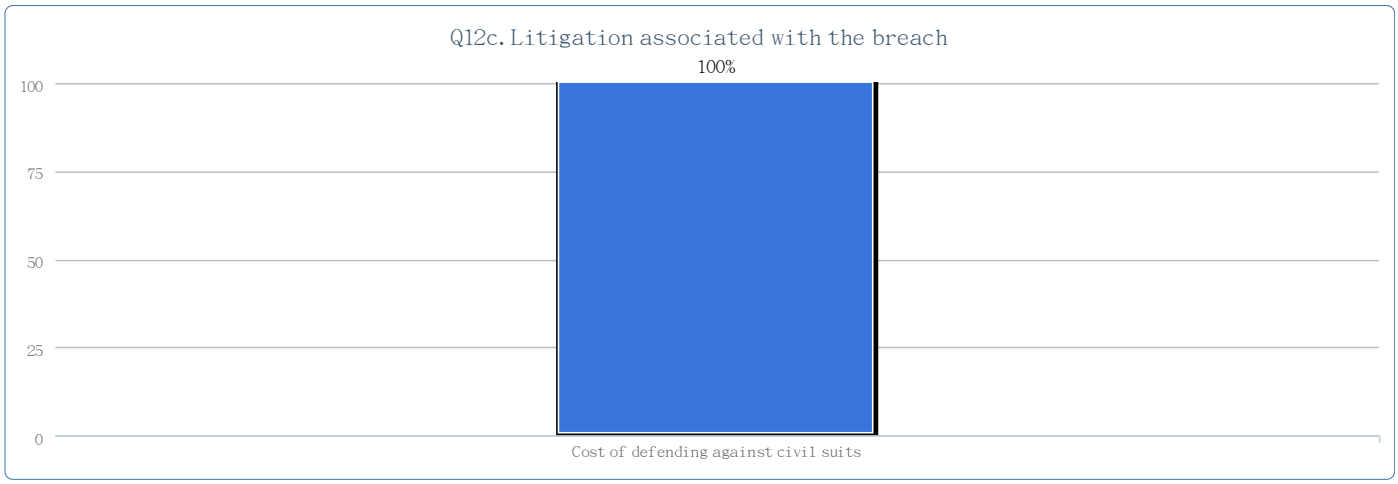
Statistics	
Total Responses	9



Q12b. External costs associated with the breach

Value	Count	Percent %
Computer Forensics	3	33.3%
Legal fees	3	33.3%
Notifications to individuals	5	55.6%
Mitigation	1	11.1%
Providing credit or identity monitoring to impacted individuals	7	77.8%

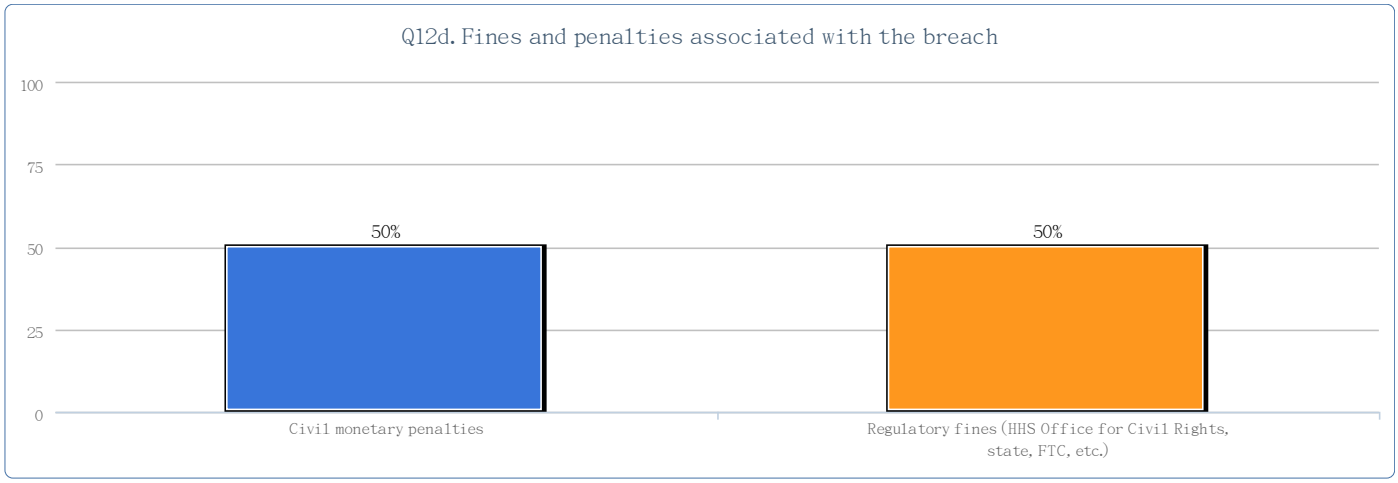
Statistics	
Total Responses	9



Q12c. Litigation associated with the breach

Value	Count	Percent %
Cost of defending against civil suits	2	100%

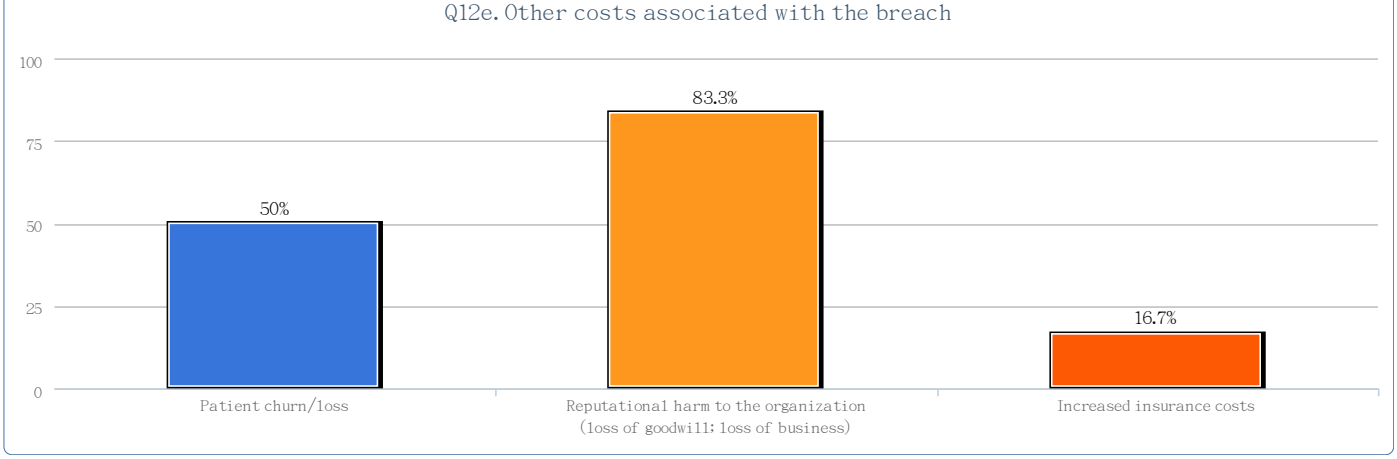
Statistics	
Total Responses	2



Q12d. Fines and penalties associated with the breach

Value	Count	Percent %
Civil monetary penalties	1	50%
Regulatory fines (HHS Office for Civil Rights, state, FTC, etc.)	1	50%

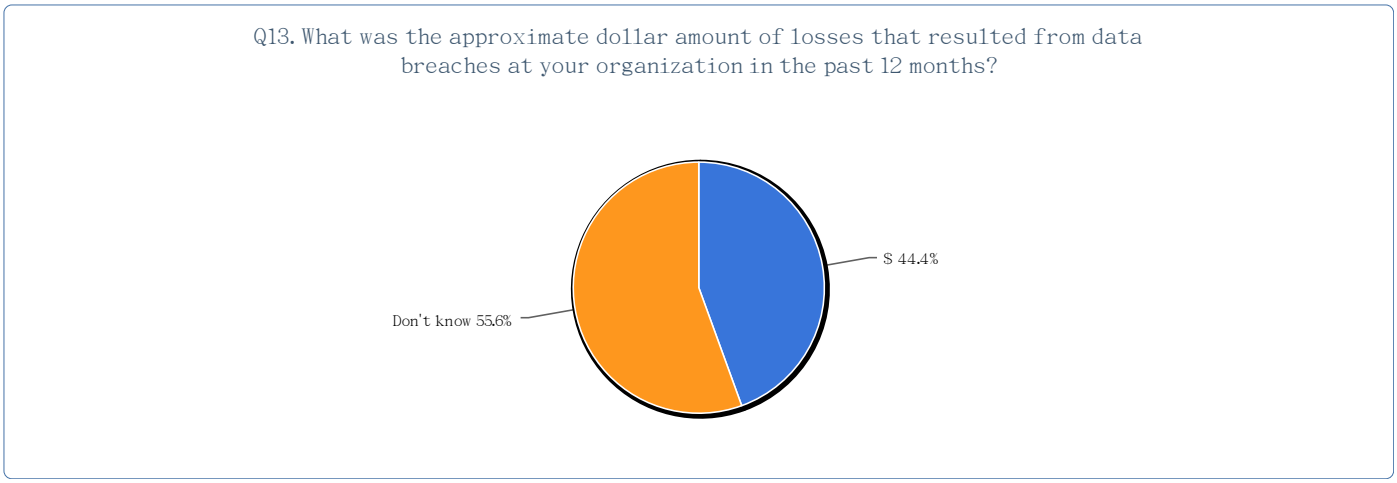
Statistics	
Total Responses	2



Q12e. Other costs associated with the breach

Value	Count	Percent %
Patient churn/loss	3	50%
Reputational harm to the organization (loss of goodwill; loss of business)	5	83.3%
Increased insurance costs	1	16.7%

Statistics	
Total Responses	6

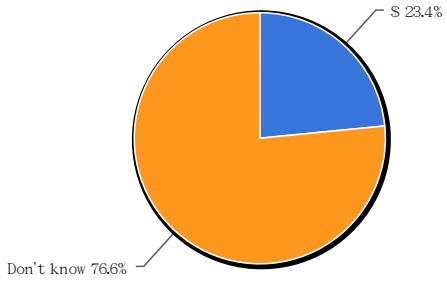


Q13. What was the approximate dollar amount of losses that resulted from data breaches at your organization in the past 12 months?

Value	Count	Percent %
$	4	44.4%
Don't know	5	55.6%

Statistics	
Total Responses	9

Q14a. Approximately, what is the estimated cost that your organization will incur to comply with HIPAA and HITECH?

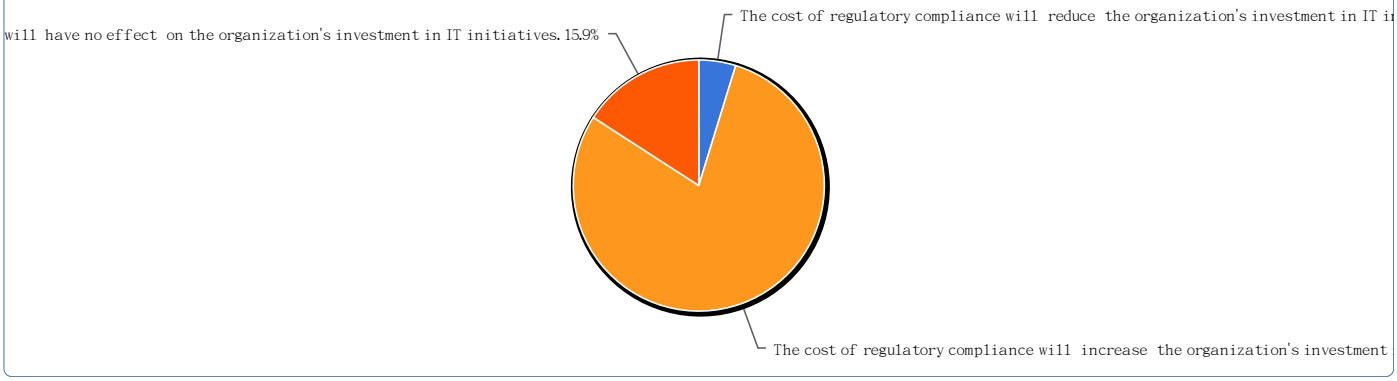


Q14a. Approximately, what is the estimated cost that your organization will incur to comply with HIPAA and HITECH?

Value	Count	Percent %
$	15	23.4%
Don't know	49	76.6%

Statistics	
Total Responses	64

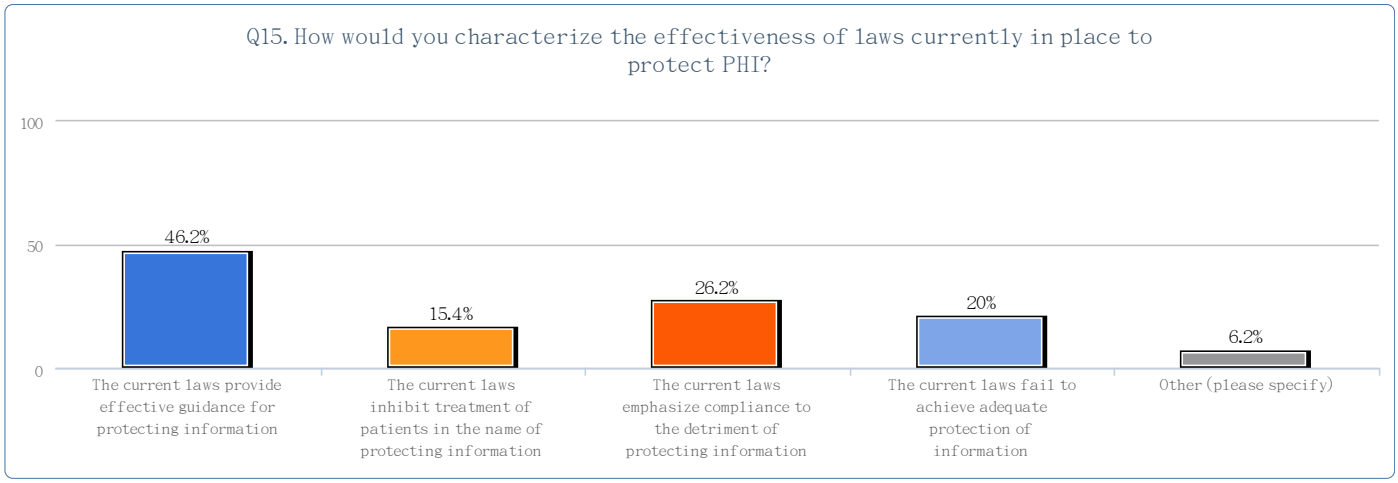
Q14b. Will the cost of regulatory compliance reduce, increase or have no effect on the organization's investment in IT initiatives? (Please select one.)



Q14b. Will the cost of regulatory compliance reduce, increase or have no effect on the organization's investment in IT initiatives? (Please select one.)

Value	Count	Percent %
The cost of regulatory compliance will reduce the organization's investment in IT initiatives.	3	4.8%
The cost of regulatory compliance will increase the organization's investment in IT initiatives.	50	79.4%
The cost of regulatory compliance will have no effect on the organization's investment in IT initiatives.	10	15.9%

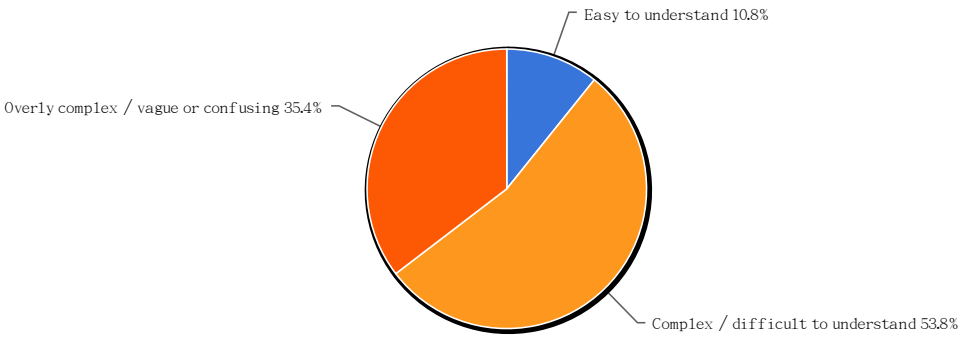
Statistics	
Total Responses	63



Q15. How would you characterize the effectiveness of laws currently in place to protect PHI?

Value	Count	Percent %
The current laws provide effective guidance for protecting information	30	46.2%
The current laws inhibit treatment of patients in the name of protecting information	10	15.4%
The current laws emphasize compliance to the detriment of protecting information	17	26.2%
The current laws fail to achieve adequate protection of information	13	20%
Other (please specify)	4	6.2%

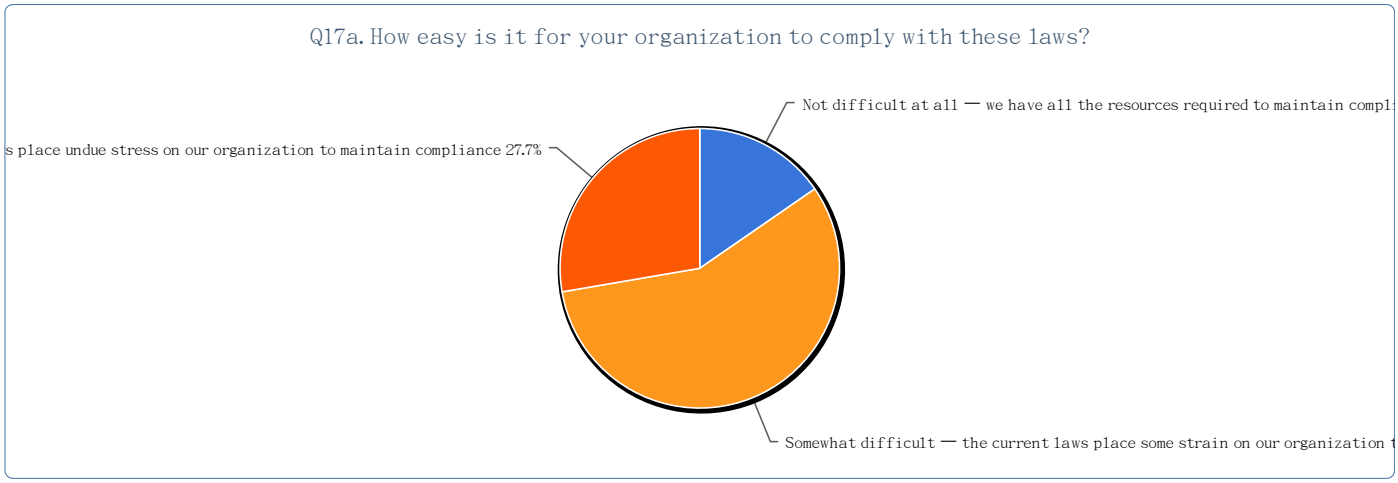
Statistics	
Total Responses	65



Q16. How would you characterize the complexity of these laws?

Value	Count	Percent %
Easy to understand	7	10.8%
Complex / difficult to understand	35	53.8%
Overly complex / vague or confusing	23	35.4%

Statistics	
Total Responses	65



Q17a. How easy is it for your organization to comply with these laws?

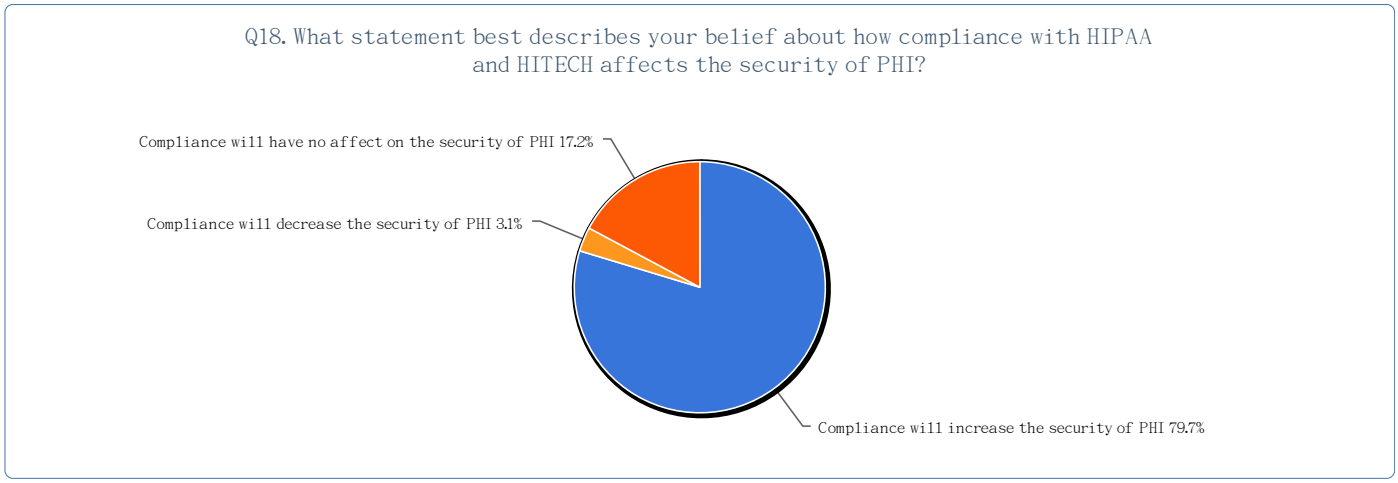
Value	Count	Percent %
Not difficult at all — we have all the resources required to maintain compliance within our organization	10	15.4%
Somewhat difficult — the current laws place some strain on our organization to maintain compliance	37	56.9%
Difficult — the current laws place undue stress on our organization to maintain compliance	18	27.7%

Statistics	
Total Responses	65

Q17b. If you answered "somewhat difficult" or "difficult" to Q17a, please briefly state why.

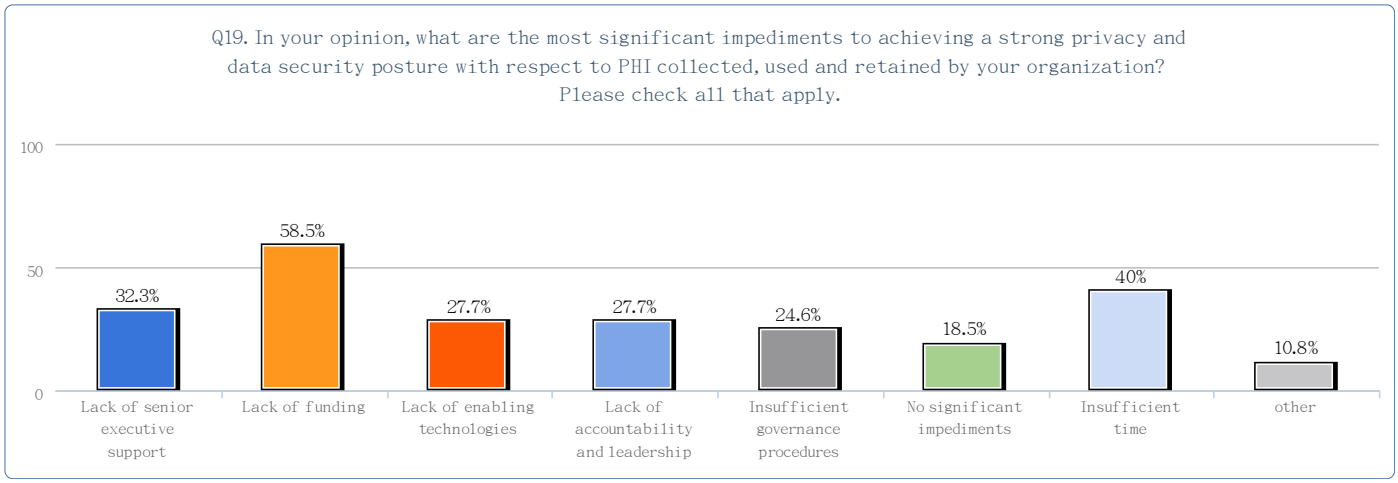
Count	Response
1	Being a smaller company, its difficult to keep up with the costs associated with what is needed.
1	Complexity and interpretation issues
1	Cost to comply
1	Lack of dedicated resources to mitigate risk.
1	Limited financial resources
1	Mix of state, federal laws, other regulations (state Insurance commissoners, PII laws)
1	Monitoring access of 9000 users is complex
1	Our systems are not set up to achieve full compliance with the regulatory requirements
1	Required outside consultation several areas of law open to interpretation
1	State and fed law conflict and add cost and confusion.
1	The challenge of ever changing tech poses risk to be in front of the changes that increase risk.
1	The laws vary by sub,ject matter, state and National.
1	The organization will not fund the necessary tools and staff to maintain compliance.
1	There is a lot of room for interpretation, no clear metrics/benchmarks exist.
1	There is so much overlap between laws that analysis is time consuming and difficult.
1	We are a small organization with very limited financial resources
1	We are intepreting more strictly than HITECH
1	We do not have the employee resources or the funds to deal with additional federal regulations.
1	We don't have a proactive breach tracking process.
1	ambiguitity in the standards..for example risk audits
1	investment in, then distribution of software/hardware to protect PHI
1	CMS documentation requirements for DME results in increased risk of breach in securing such documention from referring providers and/or patients
1	The laws are difficult to thoroughly understand and require you to view multiple documents to piece it together.
1	IN the Federal Government, there are many exclusions relating to specialized government functions and sometimes deciding if release of PHI is appropriate is difficult due to the ever changing personnel in the military

	environment.
1	simply because of the nature of healthcare, there is no one-size-fits all solution, and scalability of many products is an issue.
1	OCR tells us that we should not honor state laws that are stricter than HIPAA. They have told us to lobby our state house to change laws. We have spent an inordinate amount of time on this. They tell us we are not reading the law correctly when we say our state law is in conflict with HIPAA
1	COMPANIES WOULD ONLY BE VIGILANT ABOUT SECURITY IF DATA BREACH REALLY OCCURRED SUCH AS THEFT, FIRE ETC…
1	As a growing organization, we had minimum standrds to comply when small. The challenge is combination of complexity of electronic records and information technology as well as more complexity of HIPAA overlay with CA Welfare and Institutions codes.
1	Variability across states, and participants make is challenging to understand the various roles/suppliers affected
1	They are forcing the cost of healthcare up! Clinical personnel have to balance good patient care with rules for privacy and security.
1	Additional, dedicated resources must understand and apply laws to every aspect of the organization contiuously and repeatedly
1	State government must comply with unfunded mandates and strive to remain within budgets. Funding streams are sensitive to economic downturns.
1	For large organizations there is usually a large technology price tag that goes to security solutions rather than revenue generating solutions for the company.
1	inconsistent standards between states and feds, changing before you can implement mitigation stategies
1	The details have been unclear- for ARRA mentions security standards so we assume those apply. The DEA eprescribe standard of 2 factor authentication will be especially difficult and expensive. Also, our front end applications are fairly straightforward to manage loggs and access controls to the granular patient and data element level, but our back end data and reporting tools are much more difficult to manage in this way.
1	The nature of our services entails providing emergency assistance to travelers. On an emergency situation, it is difficult to obtained signed authorization forms.
1	Breach laws from over 40 state ,jurisdictions may have to be considered if social security numbers are involved in a breach incident. Laws requiring tracking and reporting of everyone who has touched a patient record are unworkable given most current IT systems.
1	large organization, lots of turn over, not enough time for training and awareness (too much time spent dealing with issues)
1	states laws variability lack of regulator understanding of healthcare operational processes lack of regulator understanding regarding current systems structure and lack of tools to even provide info regulators think we should provide
1	The laws have been ever changing which makes it difficult to keep pace with policies/procedures and training of employees. The process for passage often is annoying because sometimes facilities are expected to comply with the law before it is "final."
1	The lack of prescriptive requirements leave too much for interpretation. I am not asking for specific technology requirements such as encryption or DLP, simply specific statement that define what is "reasonable".
1	42CFR – The federal drug/alcohol privacy law is extremely difficult to comply with in electronic health information exchange.
1	Adequate staffing to comply with complex security screening,reporting and tracking regulations. Financial impact of additional IT oversight for security.
1	The compliance oriented nature of the healthcare industry makes it more difficult to ,justify solutions that may better protect information.
1	Have had to increase FTE's to manage new workflowds, development of software, new identity and access management applications
1	Managing medical information across different federal data use and protection regulatory schemes makes it predictable that failures will occur. State and federal laws do not align as well as they could.



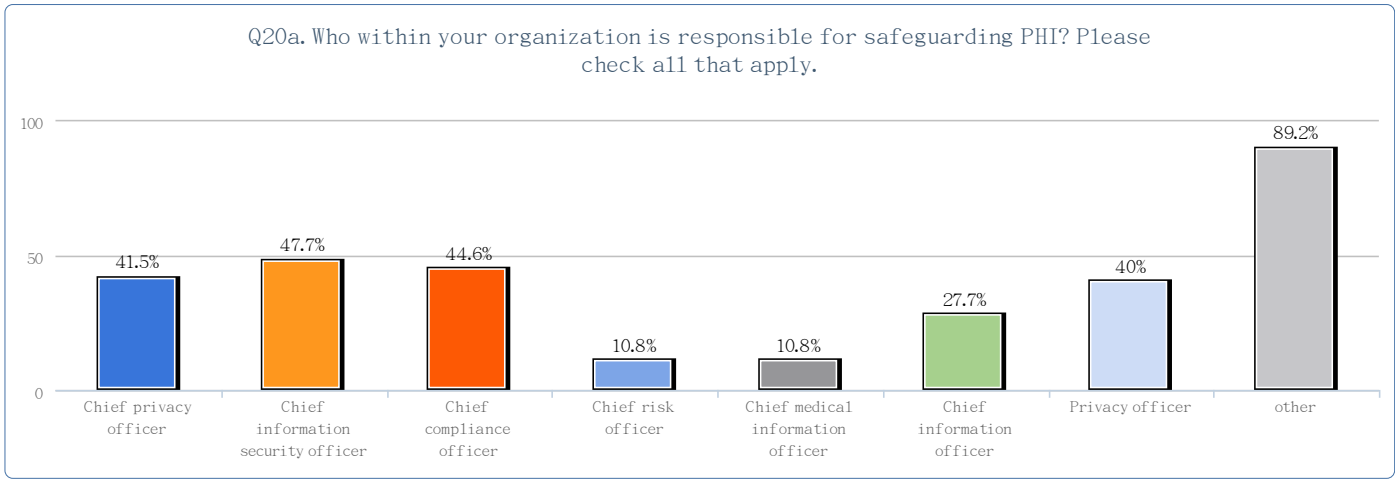
Q18. What statement best describes your belief about how compliance with HIPAA and HITECH affects the security of PHI?

Value	Count	Percent %	Statistics	
Compliance will increase the security of PHI	51	79.7%	Total Responses	64
Compliance will decrease the security of PHI	2	3.1%		
Compliance will have no affect on the security of PHI	11	17.2%		



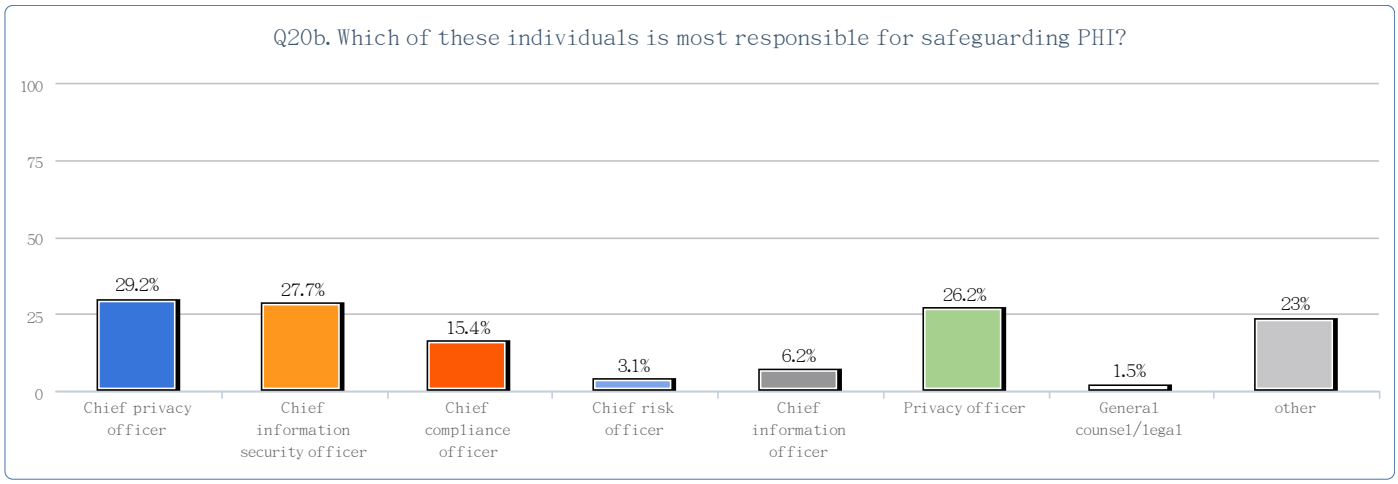
Q19. In your opinion, what are the most significant impediments to achieving a strong privacy and data security posture with respect to PHI collected, used and retained by your organization? Please check all that apply.

Value	Count	Percent %	Statistics	
Lack of senior executive support	21	32.3%	Total Responses	65
Lack of funding	38	58.5%		
Lack of enabling technologies	18	27.7%		
Lack of accountability and leadership	18	27.7%		
Insufficient governance procedures	16	24.6%		
No significant impediments	12	18.5%		
Insufficient time	26	40%		
Other (please specify)	7	10.8%		



Q20a. Who within your organization is responsible for safeguarding PHI? Please check all that apply.

Value	Count	Percent %	Statistics	
Chief privacy officer	27	41.5%	Total Responses	65
Chief information security officer	31	47.7%		
Chief compliance officer	29	44.6%		
Chief risk officer	7	10.8%		
Chief medical information officer	7	10.8%		
Chief information officer	18	27.7%		
Privacy officer	26	40%		
General counsel/legal	19	29.2%		
Human resources	11	16.9%		
Other (please specify)	18	27.7%		
No one person has overall responsibility	10	15.4%		

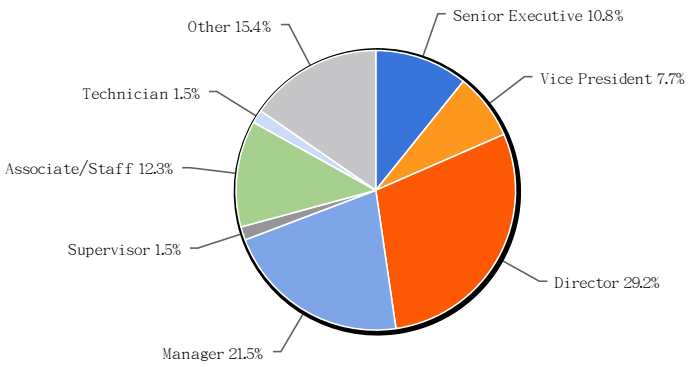


Q20b. Which of these individuals is most responsible for safeguarding PHI?

Value	Count	Percent %	Statistics	
Chief privacy officer	19	29.2%	Total Responses	65
Chief information security officer	18	27.7%		
Chief compliance officer	10	15.4%		
Chief risk officer	2	3.1%		
Chief information officer	4	6.2%		
Privacy officer	17	26.2%		
General counsel/legal	1	1.5%		
Human resources	1	1.5%		

Other (please specify)	8	12.3%
No one person has overall responsibility	6	9.2%

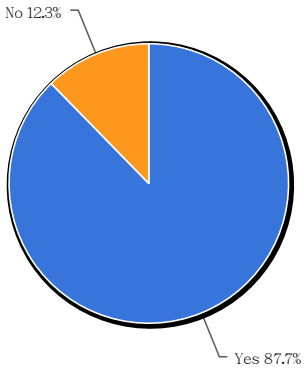
D1. What organizational level best describes your current position?



D1. What organizational level best describes your current position?

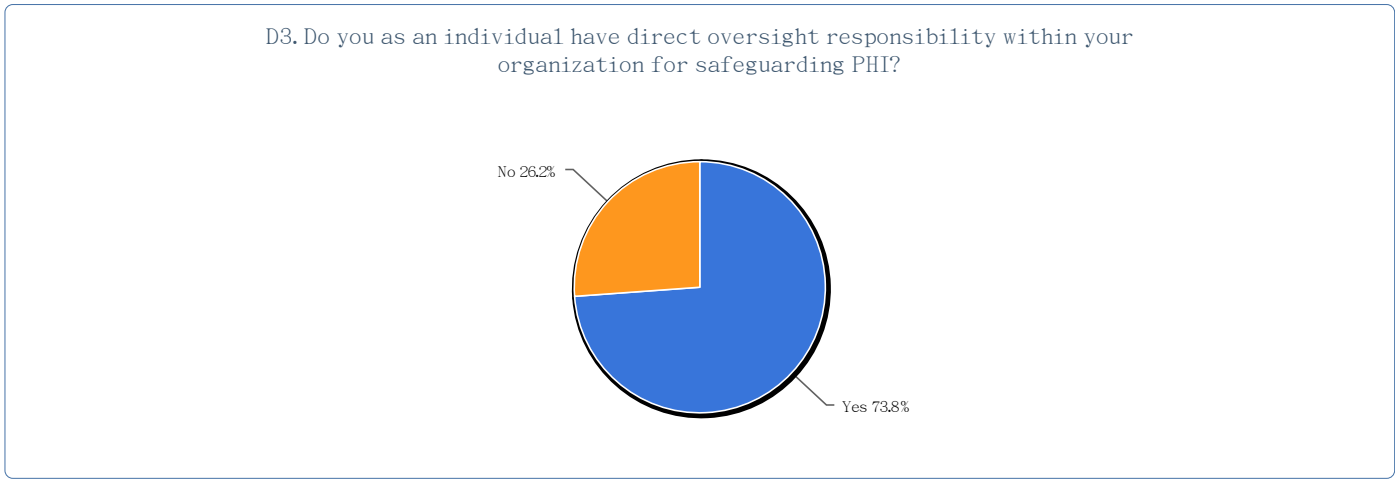
Value	Count	Percent %	Statistics	
Senior Executive	7	10.8%	Total Responses	65
Vice President	5	7.7%		
Director	19	29.2%		
Manager	14	21.5%		
Supervisor	1	1.5%		
Associate/Staff	8	12.3%		
Technician	1	1.5%		
Other	10	15.4%		

D2. Is this a full time position?



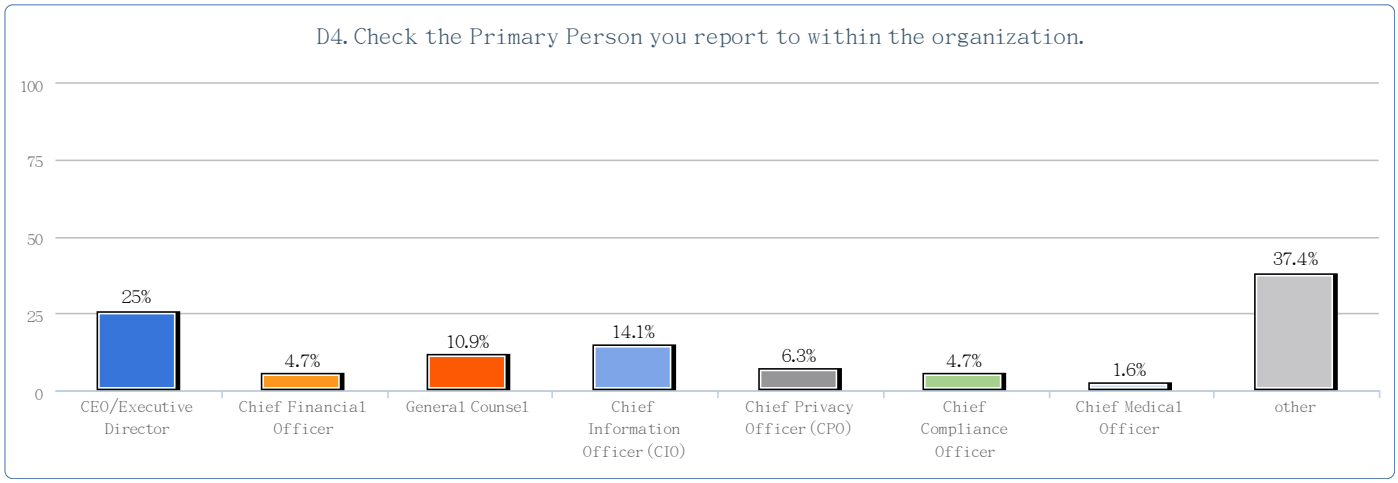
D2. Is this a full time position?

Value	Count	Percent %	Statistics	
Yes	57	87.7%	Total Responses	65
No	8	12.3%		



D3. Do you as an individual have direct oversight responsibility within your organization for safeguarding PHI?

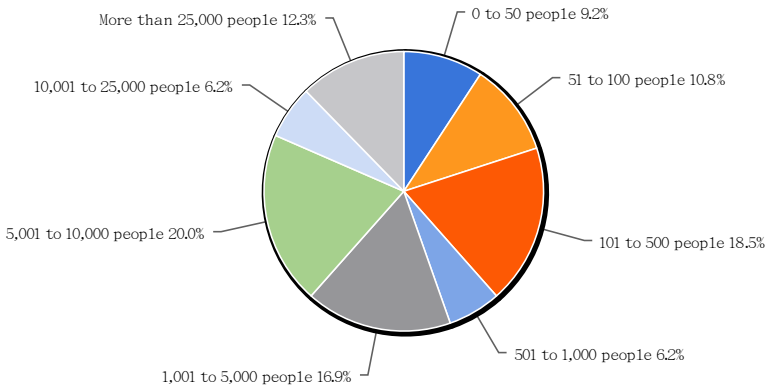
Value	Count	Percent %	Statistics	
Yes	48	73.8%	Total Responses	65
No	17	26.2%		



D4. Check the Primary Person you report to within the organization.

Value	Count	Percent %	Statistics	
CEO/Executive Director	16	25%	Total Responses	64
Chief Financial Officer	3	4.7%		
General Counsel	7	10.9%		
Chief Information Officer (CIO)	9	14.1%		
Chief Privacy Officer (CPO)	4	6.3%		
Chief Compliance Officer	3	4.7%		
Chief Medical Officer	1	1.6%		
Chief Medical Information Officer	2	3.1%		
Chief Technology Officer (CTO)	2	3.1%		
Chief Information Security Officer (CISO)	2	3.1%		
Chief Risk Officer	2	3.1%		
Other (please specify)	16	25%		

D5. What is the total headcount of your organization?

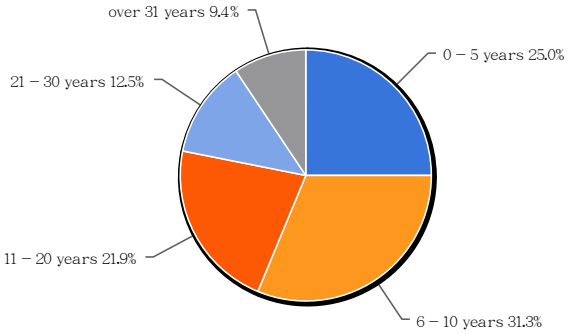


D5. What is the total headcount of your organization?

Value	Count	Percent %
0 to 50 people	6	9.2%
51 to 100 people	7	10.8%
101 to 500 people	12	18.5%
501 to 1,000 people	4	6.2%
1,001 to 5,000 people	11	16.9%
5,001 to 10,000 people	13	20%
10,001 to 25,000 people	4	6.2%
More than 25,000 people	8	12.3%

Statistics	
Total Responses	65
Sum	3,689.0
Average	72.3
StdDev	131.25
Max	501.0

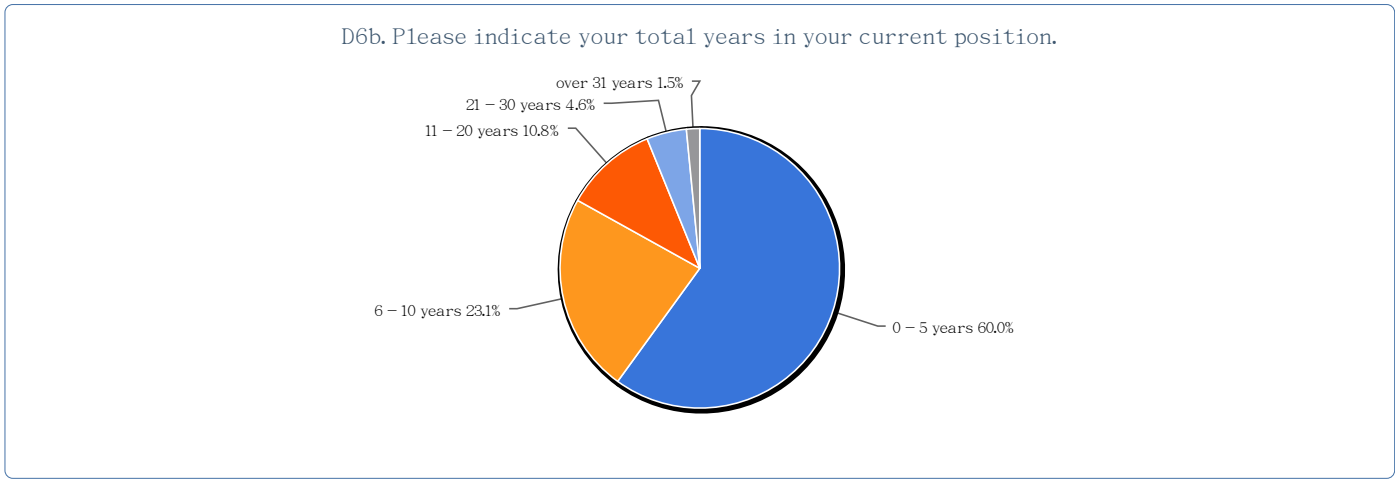
D6a. Please indicate your total years of professional experience related to safeguarding PHI.



D6a. Please indicate your total years of professional experience related to safeguarding PHI.

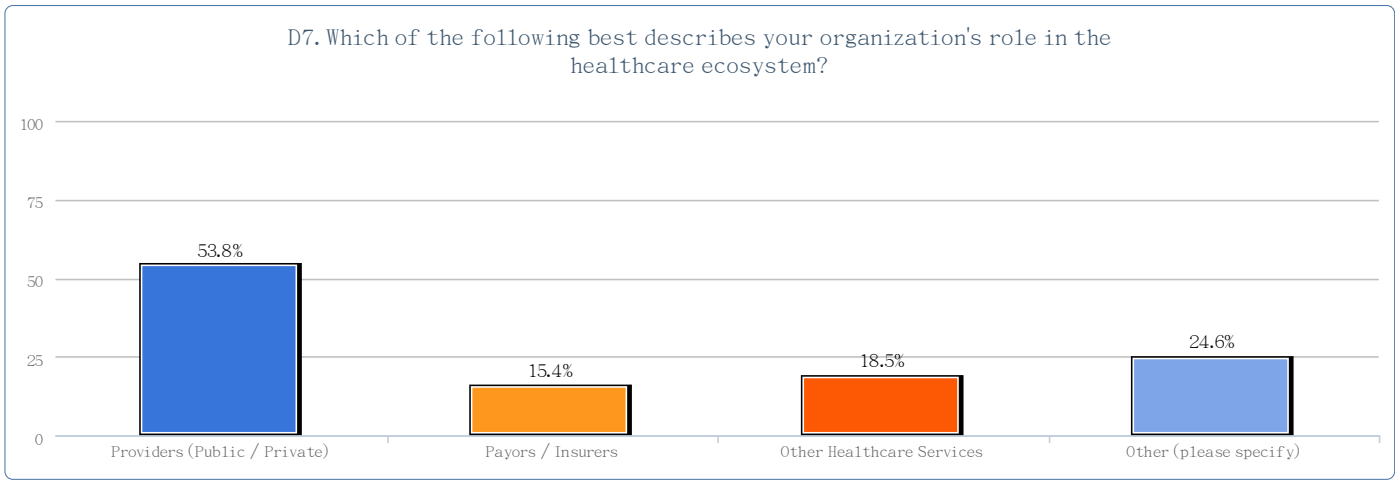
Value	Count	Percent %
0 – 5 years	16	25%
6 – 10 years	20	31.3%
11 – 20 years	14	21.9%
21 – 30 years	8	12.5%
over 31 years	6	9.4%

Statistics	
Total Responses	64
Sum	442.0
Average	10.5
StdDev	5.54
Max	21.0



D6b. Please indicate your total years in your current position.

Value	Count	Percent %	Statistics	
0 – 5 years	39	60%	Total Responses	65
6 – 10 years	15	23.1%	Sum	230.0
11 – 20 years	7	10.8%	Average	9.2
21 – 30 years	3	4.6%	StdDev	4.87
over 31 years	1	1.5%	Max	21.0



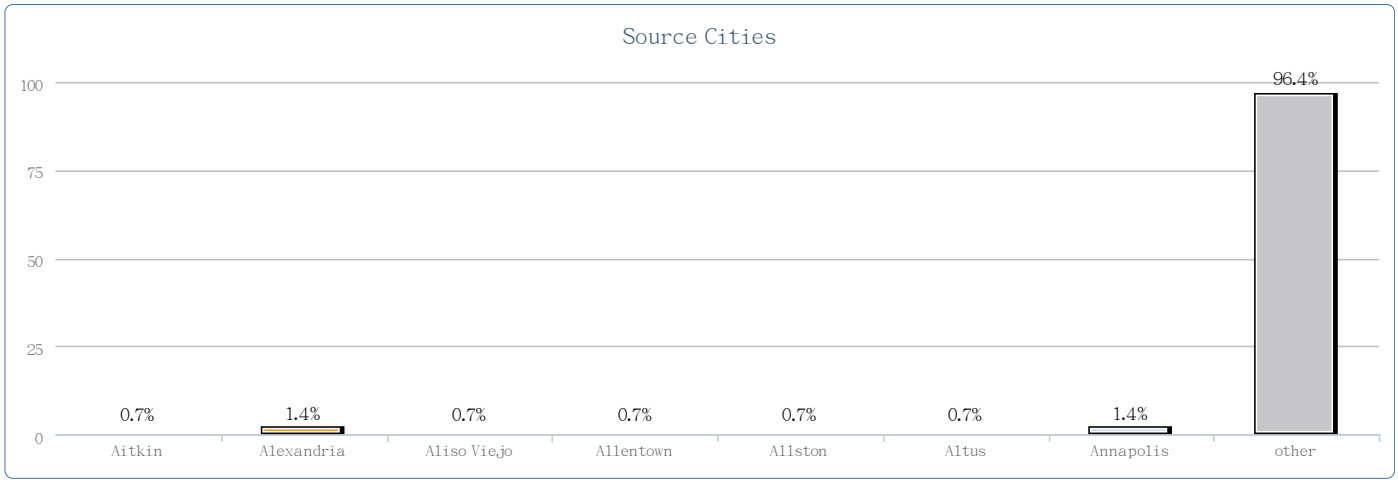
D7. Which of the following best describes your organization's role in the healthcare ecosystem?

Value	Count	Percent %	Statistics	
Providers (Public / Private)	35	53.8%	Total Responses	65
Payors / Insurers	10	15.4%		
Other Healthcare Services	12	18.5%		
Other (please specify)	16	24.6%		

What do you think of this survey? Your feedback is important to us, please tell us what you think.

Count	Response
1	Excellent survey, but I'm biased as I helped create it.
1	Excellent!
1	Good design/ vital issues
1	Good start
1	Great job!!

1	I am happy to have an opportunity to express my opinion about privacy and security in healthcare.
1	I'd like to see more of these.
1	It is detailed, clear and user friendly.
1	It seems to be intended for providers. The answers to some questions do not fit a payor.
1	It was a short but comprehensive survey.
1	It was comprehensive concerning PHI and EPHI.
1	It's OK
1	Looking forward to the results to see if they confirm our thoughts
1	Okay
1	To generic
1	Very good. Questions are easy to understand.
1	Worked well.
1	didn't drive into specifics of operational challenges that make compliance extremely difficult
1	geared specificially to PHI-engaged folks - not standard users of PHI information.
1	good questions
1	o.k. but seems to have been geared towards managers.
1	pertinent and useful
1	some of the questions needed n/a's
1	I think this is a worthwhile survey. I can't wait to see the results. Healthcare information security is behind the times. Senior leaders need to understand legacy protection mechanisms like firewalls are no longer adequate.
1	Good idea to obtain stakeholder perspective rather than ,just rhetoric. Providers and nurses should have questions specific to patient care aspects.
1	Great survey! The questions were clear and the multiple choice answers covered my answers, I only had to select "other" once and write in an answer.
1	I think it captures some interest pieces of information that would be useful in supporting a whitepaper.
1	I will be interested in learning the aggregate responses. Good survey. I think individuals will be reluctant to express concerns and issues. Some of the questions were not applicable so perhaps N/A should be an option. Also questions that I was not 100% sure about should have such a response so it does not flaw the results.
1	a couple of your questions seem more geared toward providers than payors (in particular, the ranking question)
1	Good questions that reinforce my efforts to teach my organization's leadership (my peers) and board how "quality and otucomes and marketing" is not enough without a strong compliance program.
1	I HOPE THAT THIS SURVEY WOULD BE BROUGHT UP TO MEDIA'S ATTENTION AND/ OR EVEN THE GOVERNMENT. SINCE MOST HEALTHCARE COMPANIES ARE LACKING KNOWLEDGE AND DOES NOT SEE INFORMATION SECURITY AS A BIG PLAYER IN SAFEGUARDING THE COMPANIES DATA. COMPANIES ALWAYS SEE CLINICIANS AS AN ASSET BUT DISREGARDS IT STAFF AND COMMON EMPLOYEES. I HOPE WITH THIS PROJECT , IT WOULD PUSH CEOS TO PUT BUDGET ON BUILDING AN INFORMATION SECURITY SYSTEM REGARDLESS IF ITS SMALL OR BIG. I HOPE THIS PROJECT WOULD BE SUCCESSFUL!!!! I HAVE BEEN WAITING FOR THIS THING TO HAPPEN. I HOPE THIS PROJECT WOULD SUCCEED IN ITS ENDEAVOR.
1	Depends on who you send the results too. If you send them to congress and they listen maybe they will implement stricter rules to protect PHI. With today's technology and sharing of data, no ones PHI is protected anymore.
1	Having worked on this project, I'm not sure the questions will get you the infomation you wanted, particularly about the costs of a breach.
1	I do not understand how these specific questions will lead to analysis of the level of harm. They are more directed toward preparedness to safeguard. I answer these kinds of surveys an average of 1/mth. I am interested in the harm to individual issue and would have liked to see a more direct link.



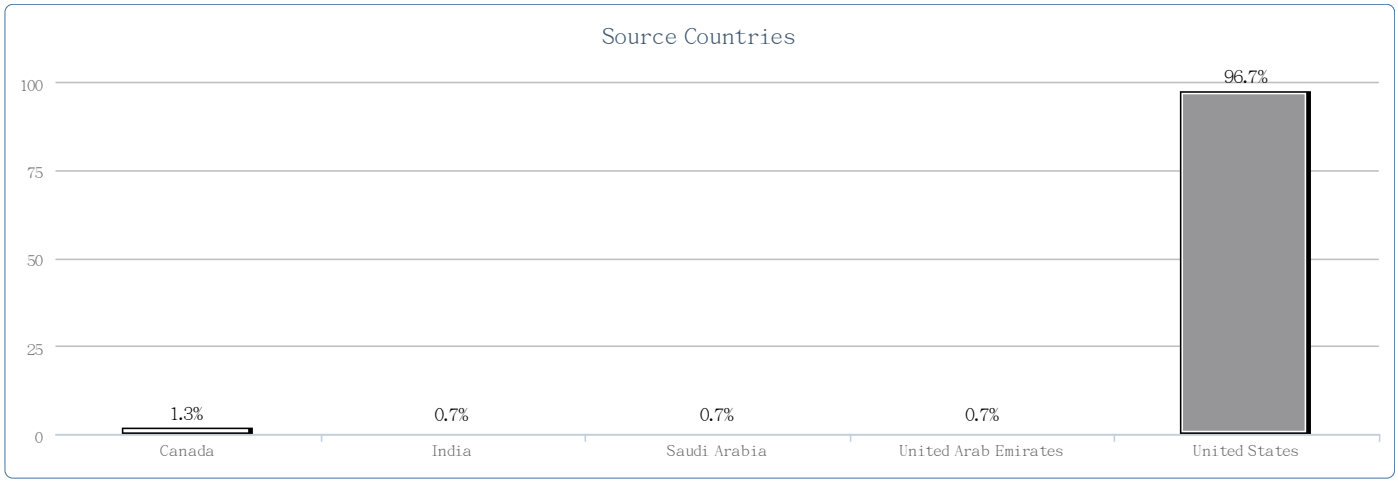
Source Cities

Value	Count	Percent %
Aitkin	1	0.7%
Alexandria	2	1.4%
Aliso Viejo	1	0.7%
Allentown	1	0.7%
Allston	1	0.7%
Altus	1	0.7%
Annapolis	2	1.4%
Arlington	1	0.7%
Arvada	1	0.7%
Baltimore	2	1.4%
Baton Rouge	2	1.4%
Bethesda	1	0.7%
Biloxi	1	0.7%
Blue Springs	1	0.7%
Bozeman	1	0.7%
Brentwood	1	0.7%
Bristol	1	0.7%
Buffalo	1	0.7%
Cambridge	1	0.7%
Carrollton	1	0.7%
Cedar Park	1	0.7%
Chatham	1	0.7%
Chesaning	1	0.7%
Chicago	1	0.7%
Cleveland	1	0.7%
Columbia	1	0.7%
Columbus	1	0.7%
Culver City	1	0.7%
Dearborn	1	0.7%
Denver	1	0.7%
Des Plaines	1	0.7%
Dubai	1	0.7%
Duluth	1	0.7%
East Elmhurst	1	0.7%
El Monte	1	0.7%
Elizabethtown	2	1.4%

Statistics	
Total Responses	148

Everett	2	1.4%
Fairport	1	0.7%
Foster City	1	0.7%
Franklin	2	1.4%
Gainesville	1	0.7%
Gillette	1	0.7%
Gonzales	1	0.7%
Grand Ronde	1	0.7%
Harrington	1	0.7%
Herndon	1	0.7%
Herrin	1	0.7%
Houston	4	2.7%
Jersey City	2	1.4%
John Day	1	0.7%
La Crosse	1	0.7%
Lewes	1	0.7%
Los Angeles	2	1.4%
Macon	1	0.7%
Madison	1	0.7%
Madison Heights	1	0.7%
Markham	1	0.7%
Mcdonough	1	0.7%
Medford	1	0.7%
Mesa	1	0.7%
Minneapolis	8	5.4%
Morganton	1	0.7%
Morrisville	1	0.7%
Mountain View	1	0.7%
Napa	1	0.7%
Nashville	2	1.4%
New York	2	1.4%
Newark	1	0.7%
Nixa	1	0.7%
Novato	1	0.7%
Oakland	2	1.4%
Oldsmar	1	0.7%
Olney	1	0.7%
Omaha	1	0.7%
Orlando	2	1.4%
Pacifica	1	0.7%
Palo Alto	1	0.7%
Pittsburgh	1	0.7%
Plainsboro	1	0.7%
Pollok	3	2%
Port Saint Lucie	1	0.7%
Portland	3	2%
Poulsbo	1	0.7%
Prescott	1	0.7%
Providence	1	0.7%
Provincetown	2	1.4%
Pune	1	0.7%

Puyallup	1	0.7%
Reston	1	0.7%
Riyadh	1	0.7%
Rochester	4	2.7%
Rockville	1	0.7%
Rutland	1	0.7%
Saint Paul	6	4.1%
San Antonio	1	0.7%
San Diego	1	0.7%
San Jose	3	2%
Shelton	1	0.7%
Southfield	1	0.7%
Sunnyvale	1	0.7%
Sussex	1	0.7%
Topeka	1	0.7%
Tulsa	1	0.7%
Vancouver	1	0.7%
Warfordsburg	1	0.7%
Washington	3	2%
Winston Salem	2	1.4%



Source Countries

Value	Count	Percent %
Canada	2	1.3%
India	1	0.7%
Saudi Arabia	1	0.7%
United Arab Emirates	1	0.7%
United States	146	96.7%

Statistics	
Total Responses	151