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.

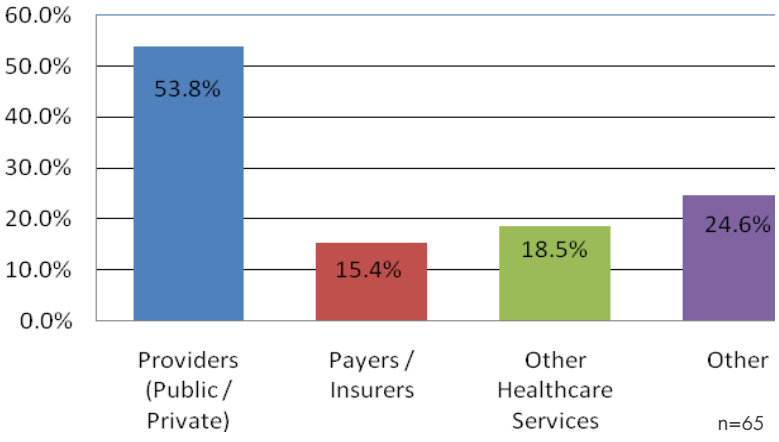


Figure 1 - Participant Role in the Health Care Ecosystem

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.

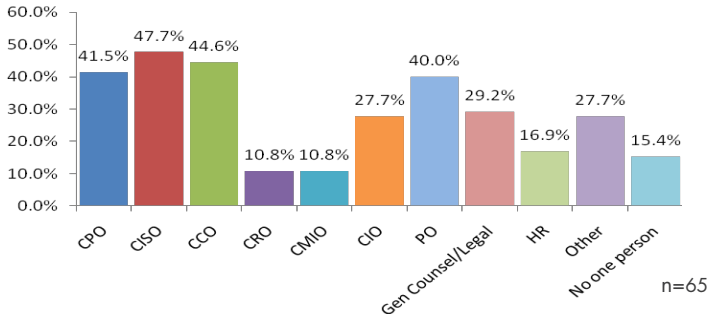


Figure 2 - Overall responsibility for Safeguarding PHI

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.

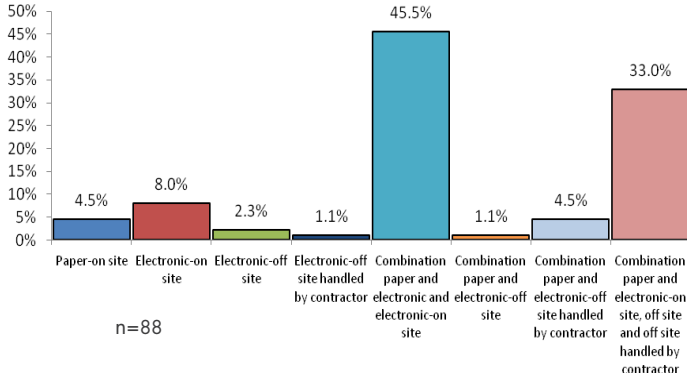


Figure 3 - Type of Records Management by Organization

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%).

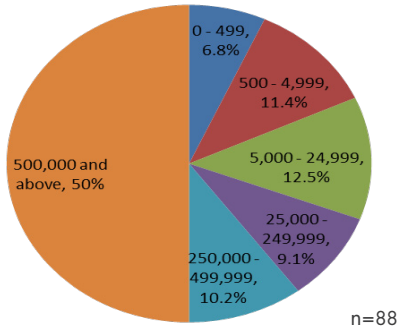


Figure 4 - PHI Survey - Number of PHI Records Responsible for by Organization

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.

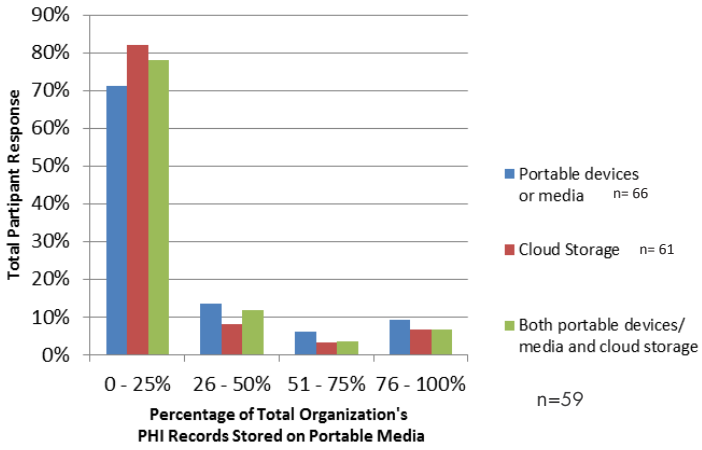


Figure 5 - Percent of Records Managed on Portable Media

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.

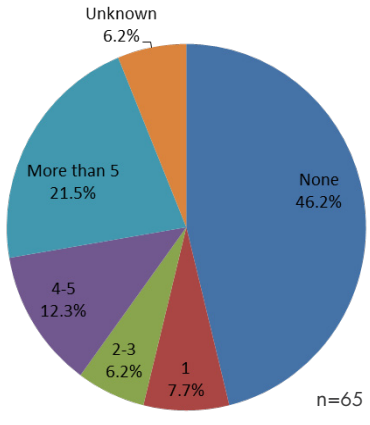


Figure 6 - Number of Breaches Suffered by Organization in Prior 12-Month Period

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.

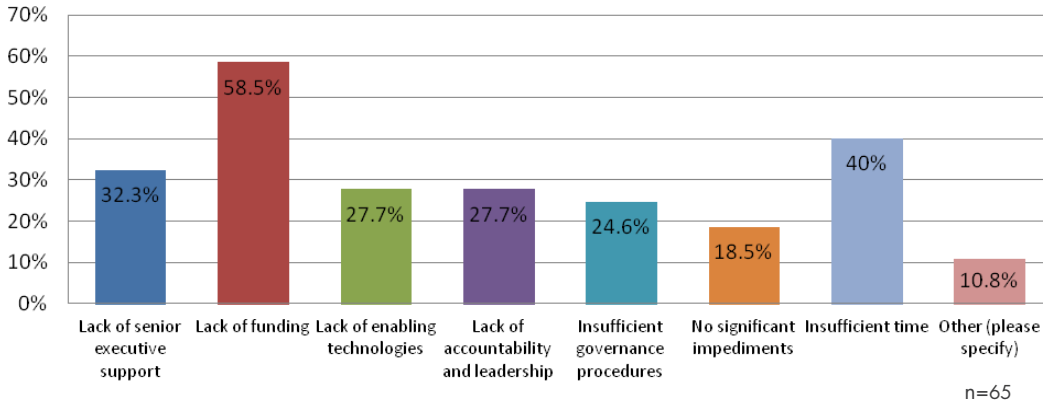


Figure 7 - Most Significant Impediments to Achieving a Strong Privacy and Data Security

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?

		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Electronic format	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?

		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Paper form	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?

		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
Both electronic and paper	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?

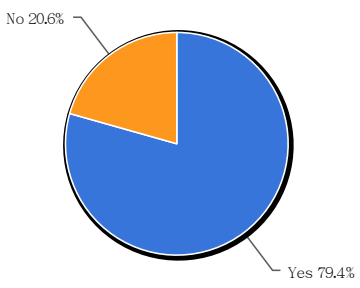
		Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?						
		None (skip to Q14)	1	2 – 3	4 – 5	More than 5	Don't know	Totals
D1. What organizational	Senior Executive	6 85.7% 20.0%	1 14.3% 20.0%	0 0.0% 0.0%	0 0.0% 0.0%	0 0.0% 0.0%	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
	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
	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
	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
	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
	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
	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
	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?

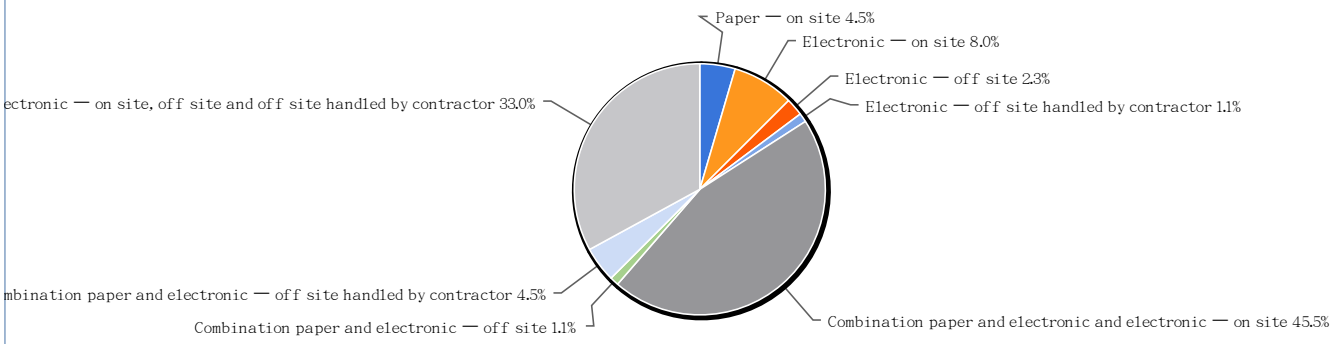


S1. Is your organization responsible for the collection, use, storage, or sharing of PHI, or does your organization contract with a third party to collect, store, use or share PHI?

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)?

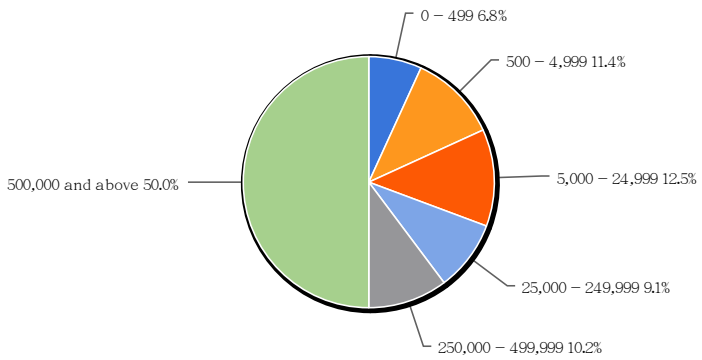


S2. Which of the below PHI records management descriptions best describes your organization (select one)?

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.

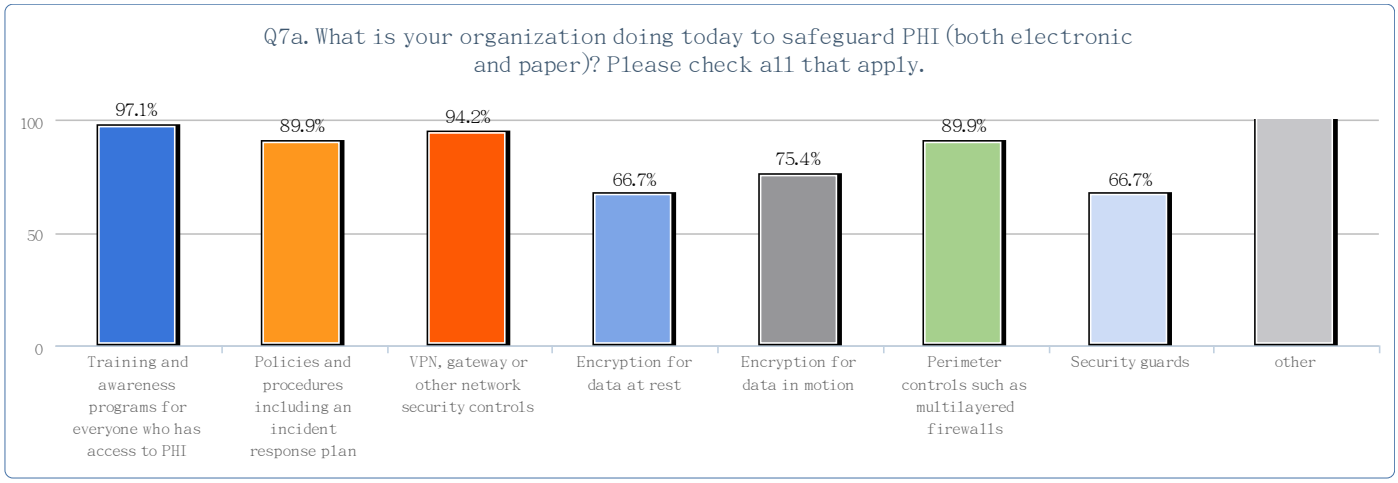
Q6a. What do you see as the mostly likely current threats that may affect your organization's ability to secure PHI?

	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%

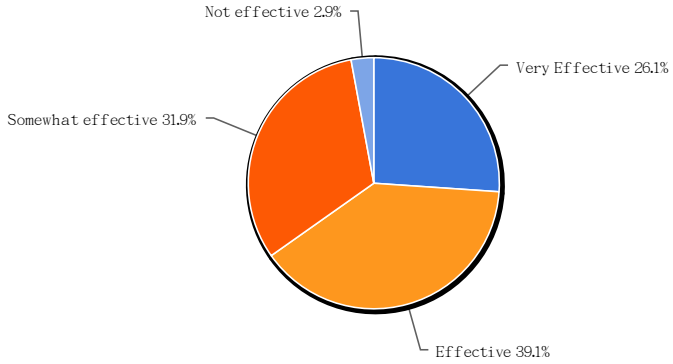


Q7a. What is your organization doing today to safeguard PHI (both electronic and paper)? Please check all that apply.

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?

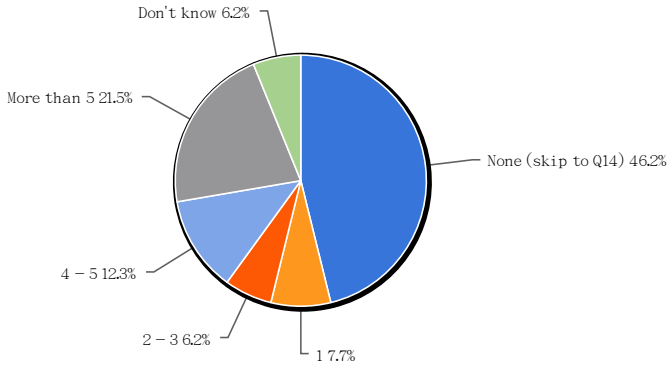


Q7b. How would you rate the effectiveness of the above mentioned data security measures you have in-place for securing PHI?

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?

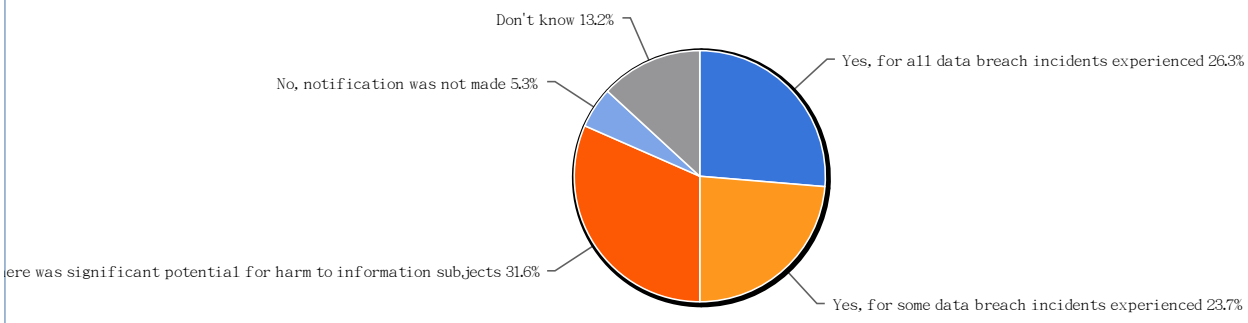


Q8. How many data breaches involving the exposure, loss or theft of PHI has your organization experienced in the past 12 months?

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?

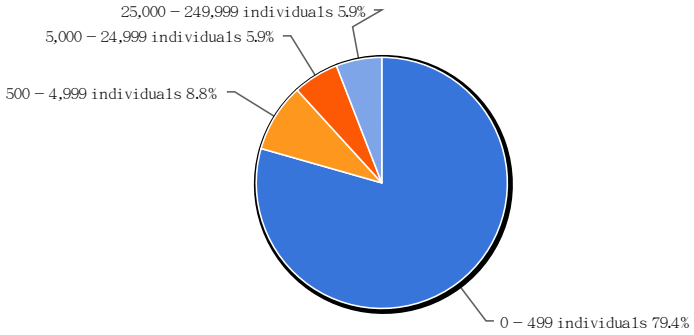


Q9. Did your organization notify individuals whose information was breached in the past 12 months?

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

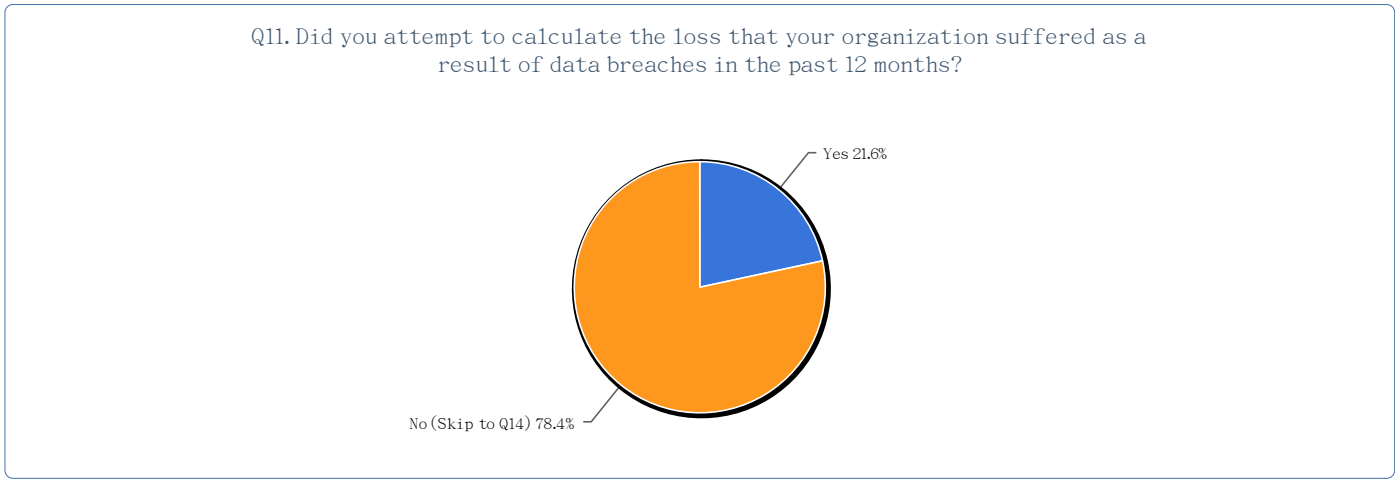
Q10. Approximately, how many individuals were impacted as a result of all data breaches experienced in the past 12 months?



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%

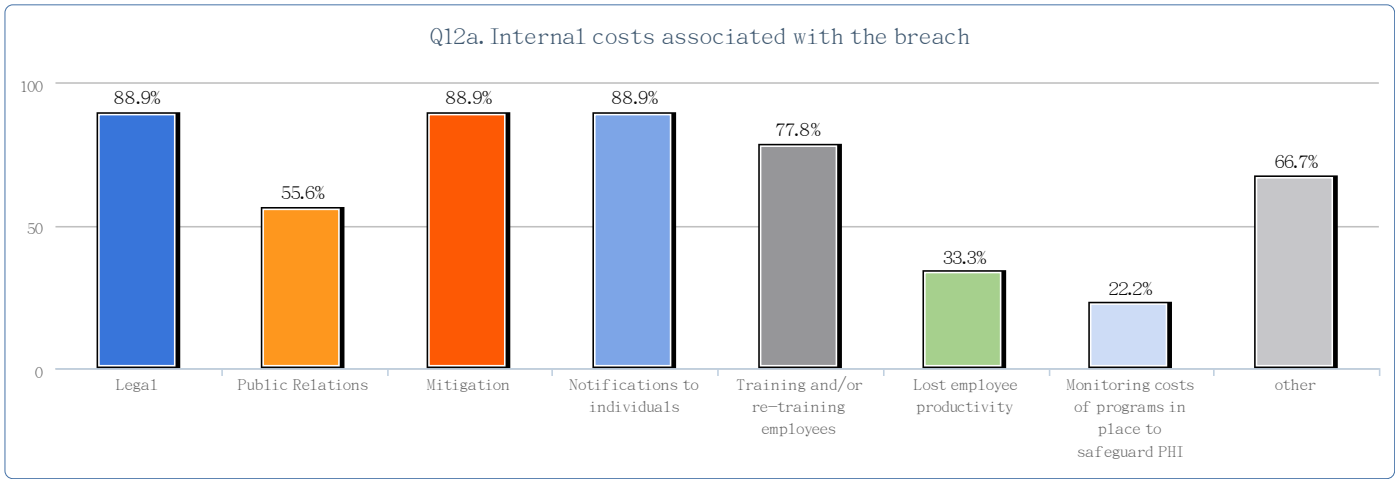
Statistics	
Total Responses	34
Sum	1,560.0
Average	222.9
StdDev	240.13
Max	500.0



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%

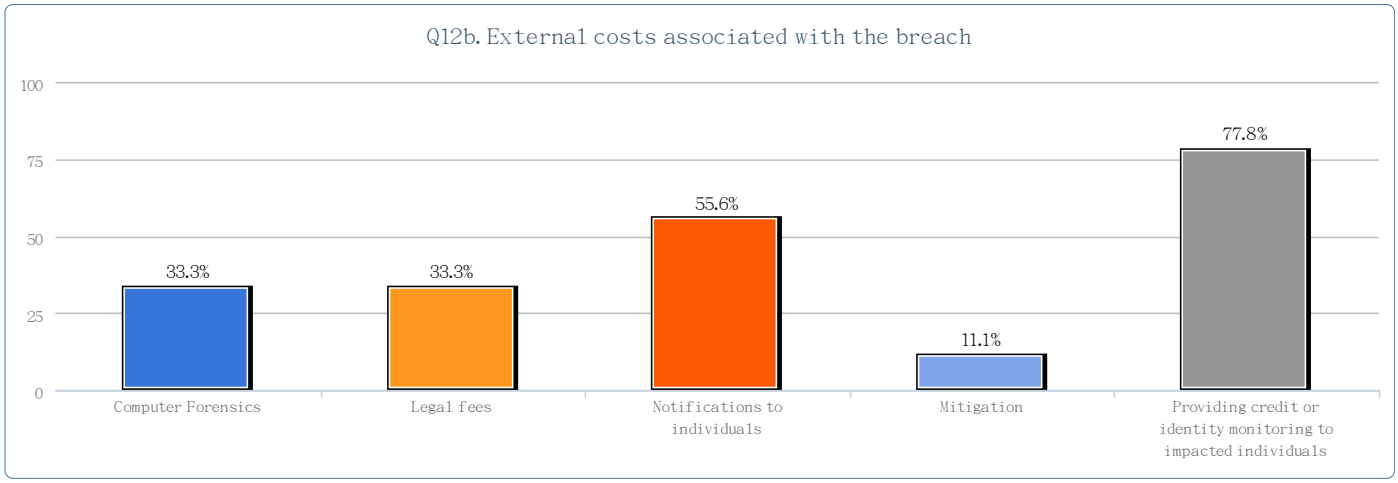
Statistics	
Total Responses	37



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%

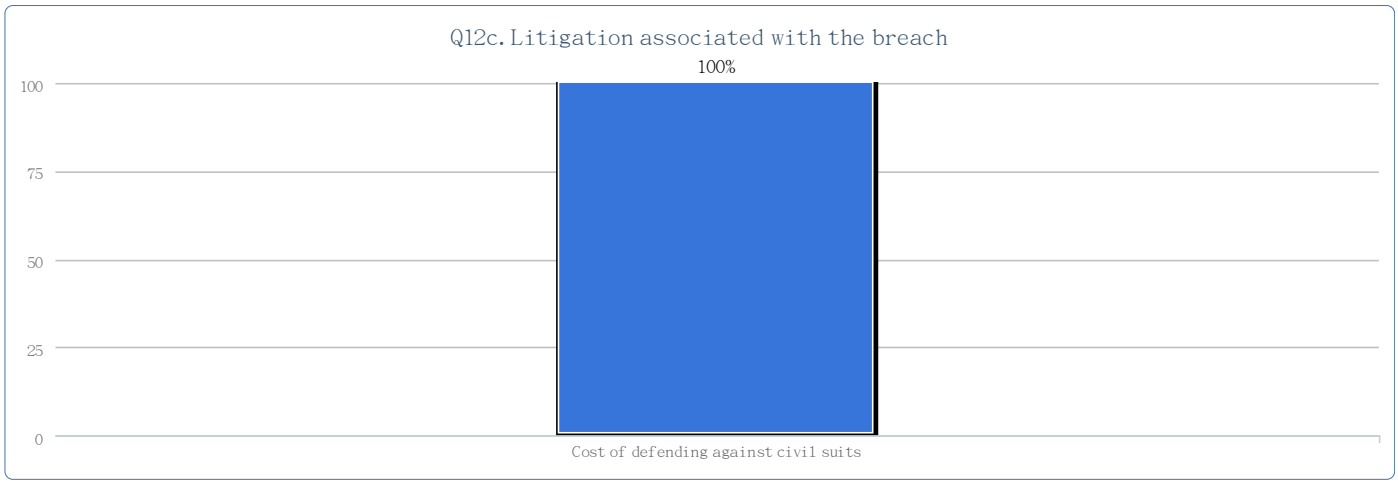
Statistics	
Total Responses	9



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%

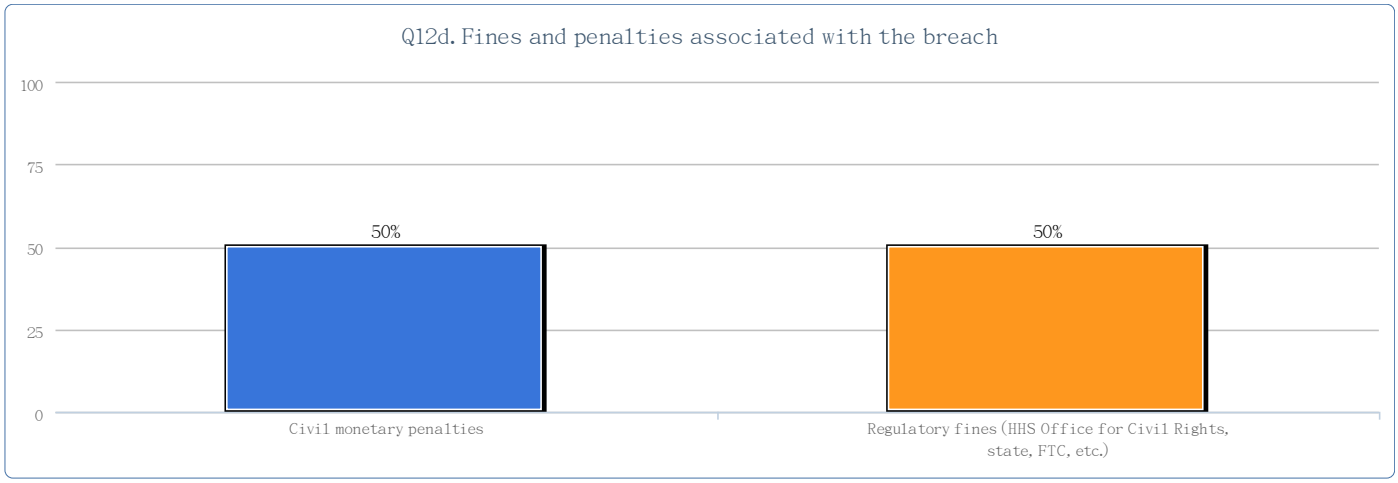
Statistics	
Total Responses	9



Q12c. Litigation associated with the breach

Value	Count	Percent %
Cost of defending against civil suits	2	100%

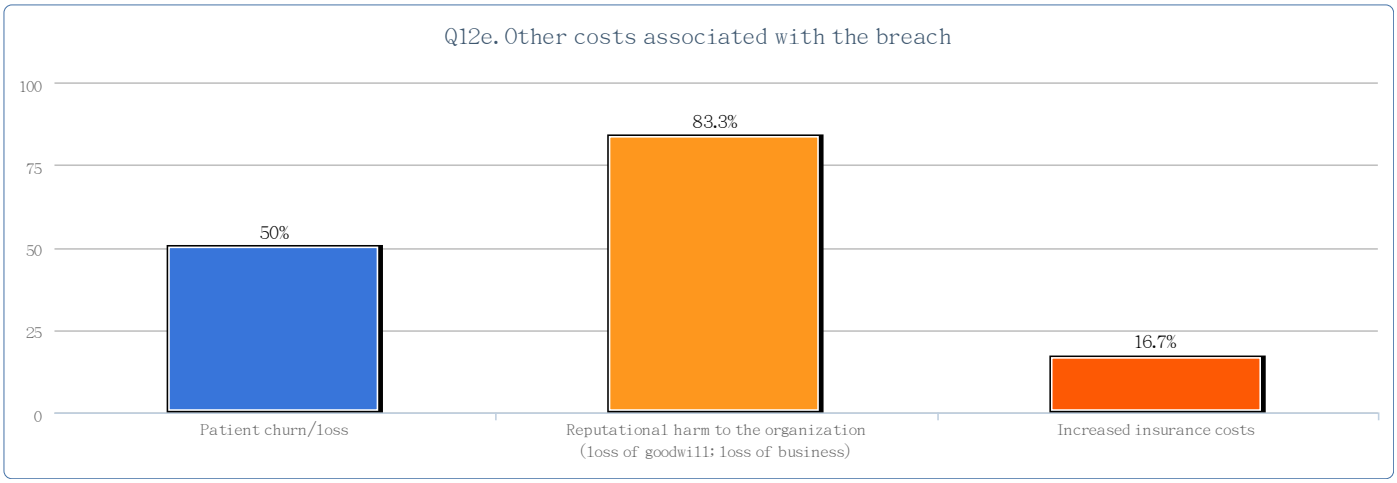
Statistics	
Total Responses	2



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%

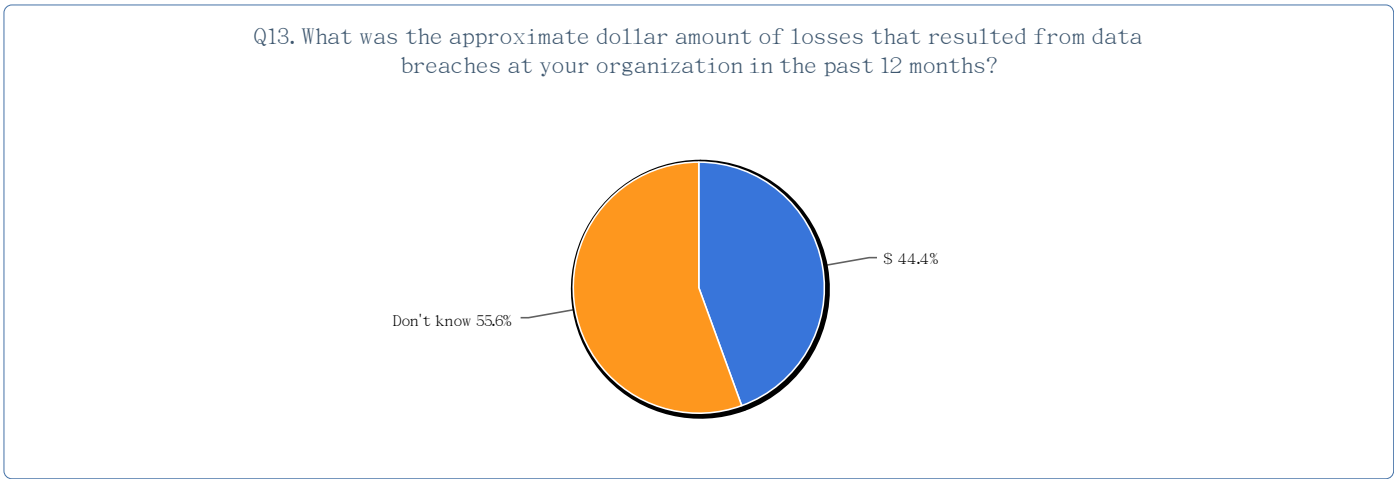
Statistics	
Total Responses	2



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

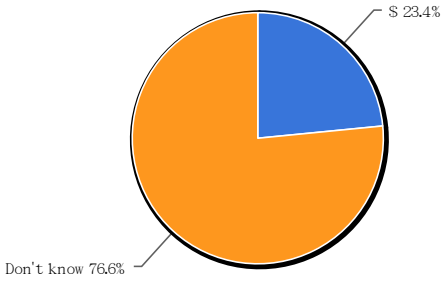


Q13. What was the approximate dollar amount of losses that resulted from data breaches at your organization in the past 12 months?

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?

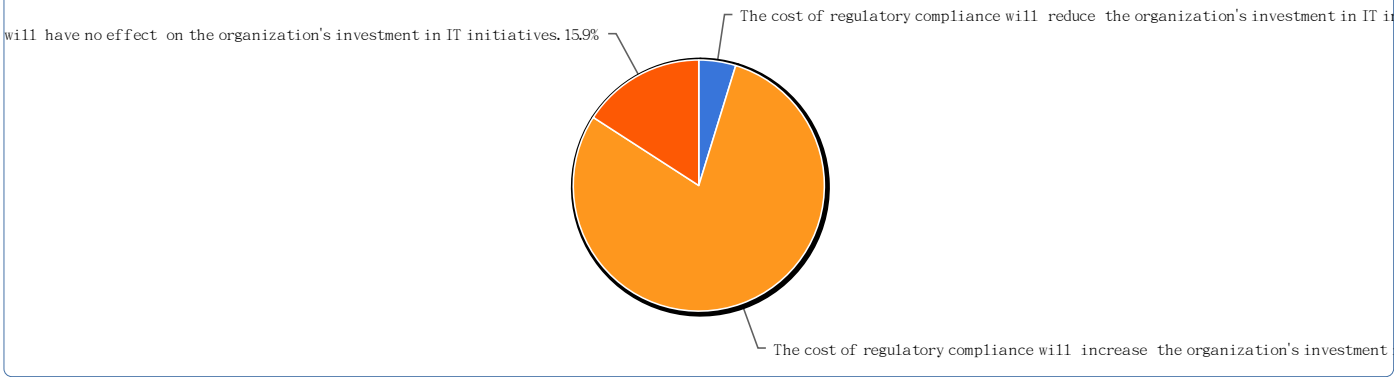


Q14a. Approximately, what is the estimated cost that your organization will incur to comply with HIPAA and HITECH?

Value	Count	Percent %
$	15	23.4%
Don't know	49	76.6%

Statistics	
Total Responses	64

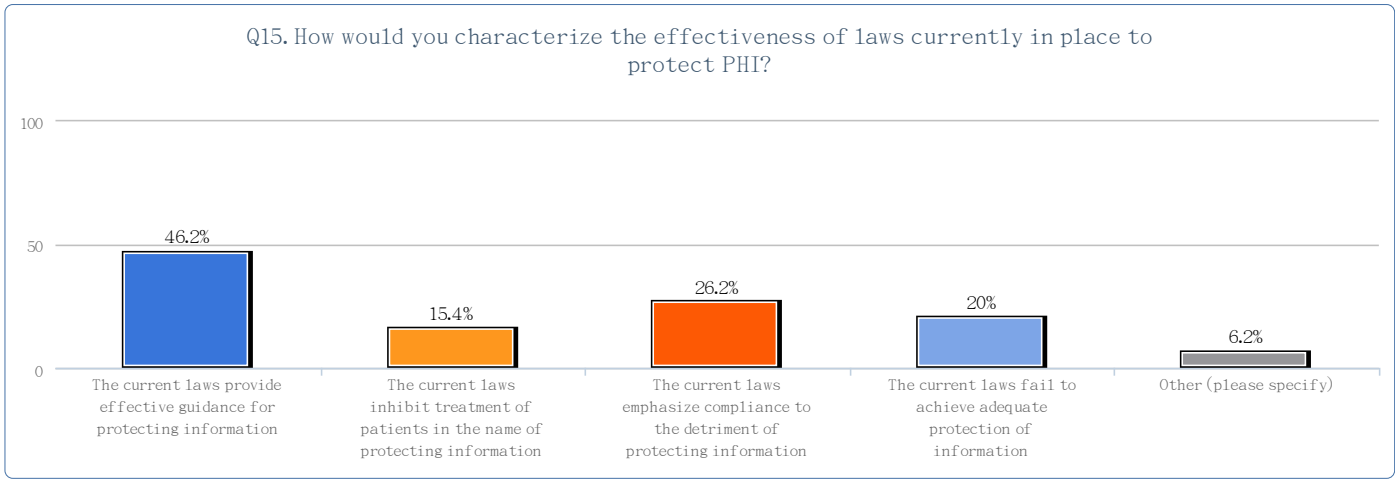
Q14b. Will the cost of regulatory compliance reduce, increase or have no effect on the organization's investment in IT initiatives? (Please select one.)



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%

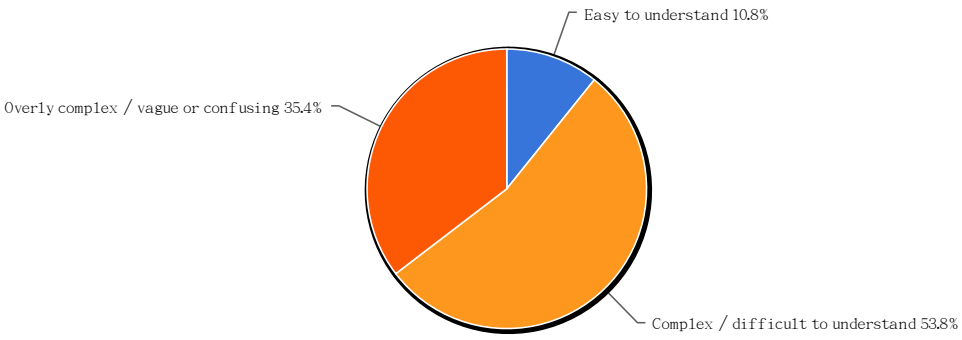
Statistics	
Total Responses	63



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%

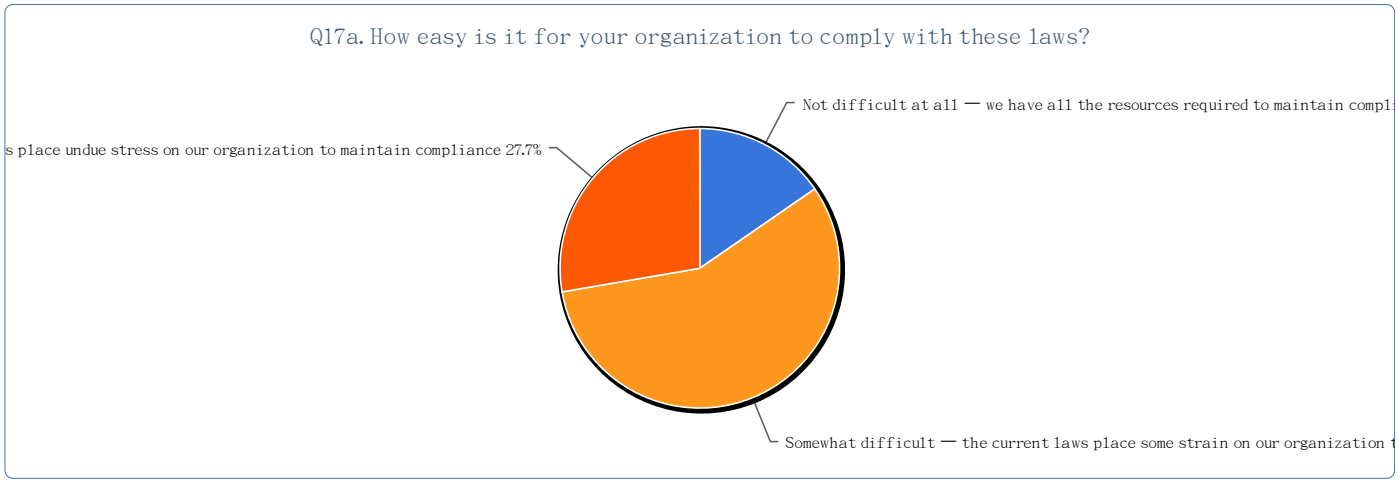
Statistics	
Total Responses	65



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?

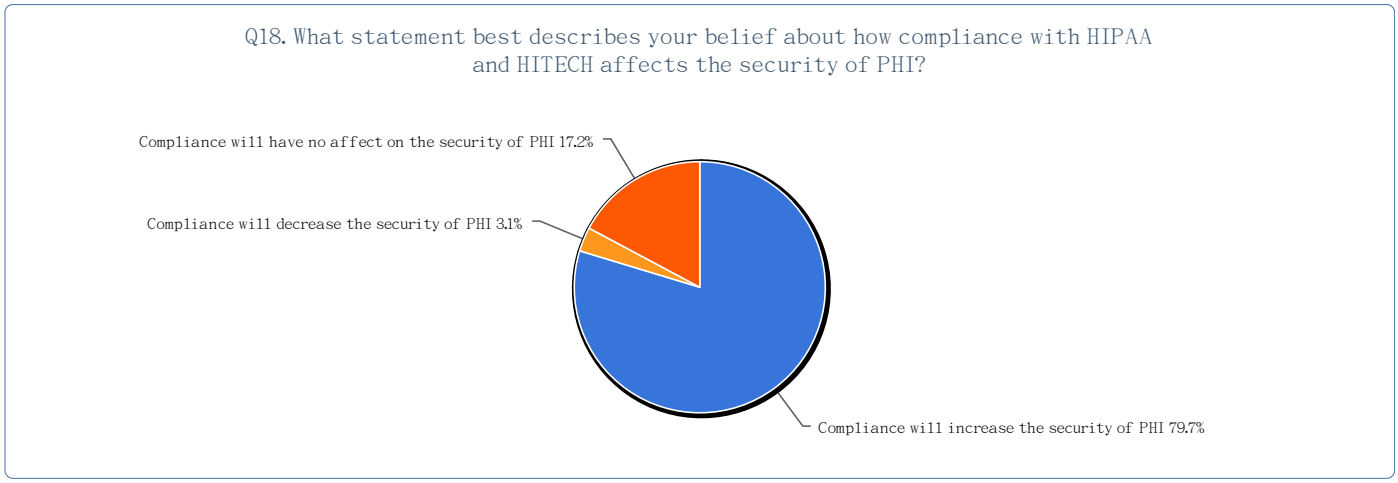
Value	Count	Percent %
Not difficult at all — we have all the resources required to maintain compliance within our organization	10	15.4%
Somewhat difficult — the current laws place some strain on our organization to maintain compliance	37	56.9%
Difficult — the current laws place undue stress on our organization 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

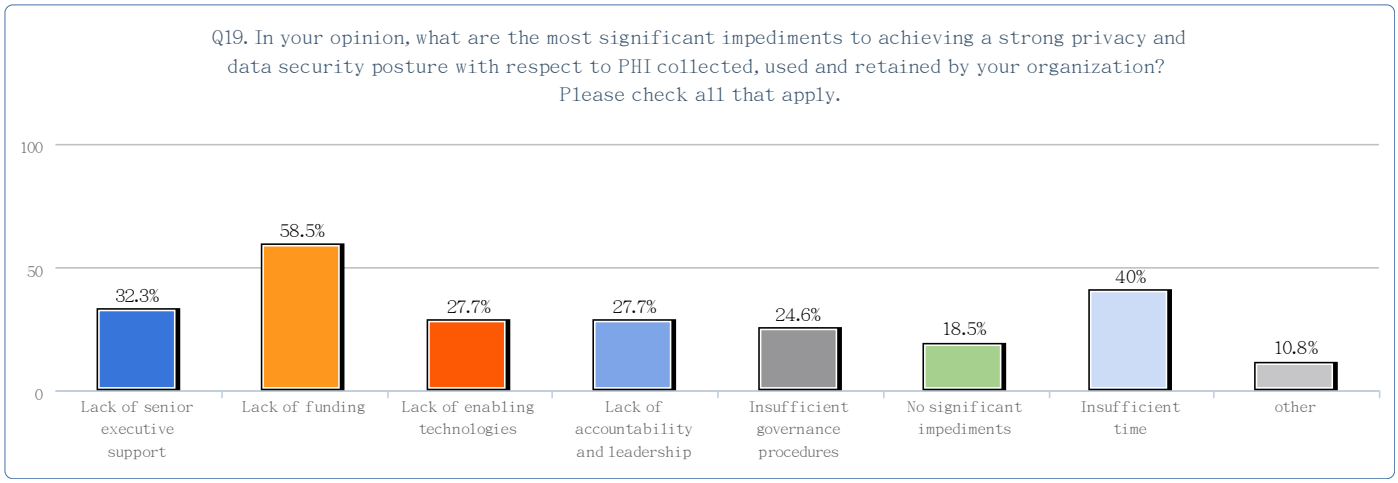
	environment.
1	simply because of the nature of healthcare, there is no one-size-fits all solution, and scalability of many products is an issue.
1	OCR tells us that we should not honor state laws that are stricter than HIPAA. They have told us to lobby our state house to change laws. We have spent an 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 %
Compliance will increase the security of PHI	51	79.7%
Compliance will decrease the security of PHI	2	3.1%
Compliance will have no affect on the security of PHI	11	17.2%

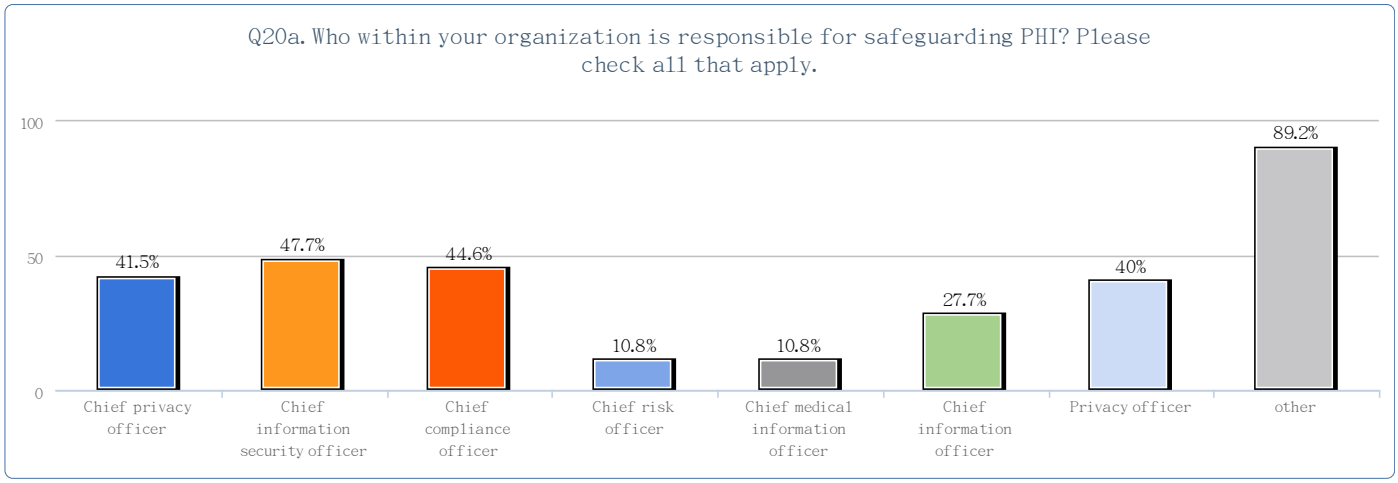
Statistics	
Total Responses	64



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 %
Lack of senior executive support	21	32.3%
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%

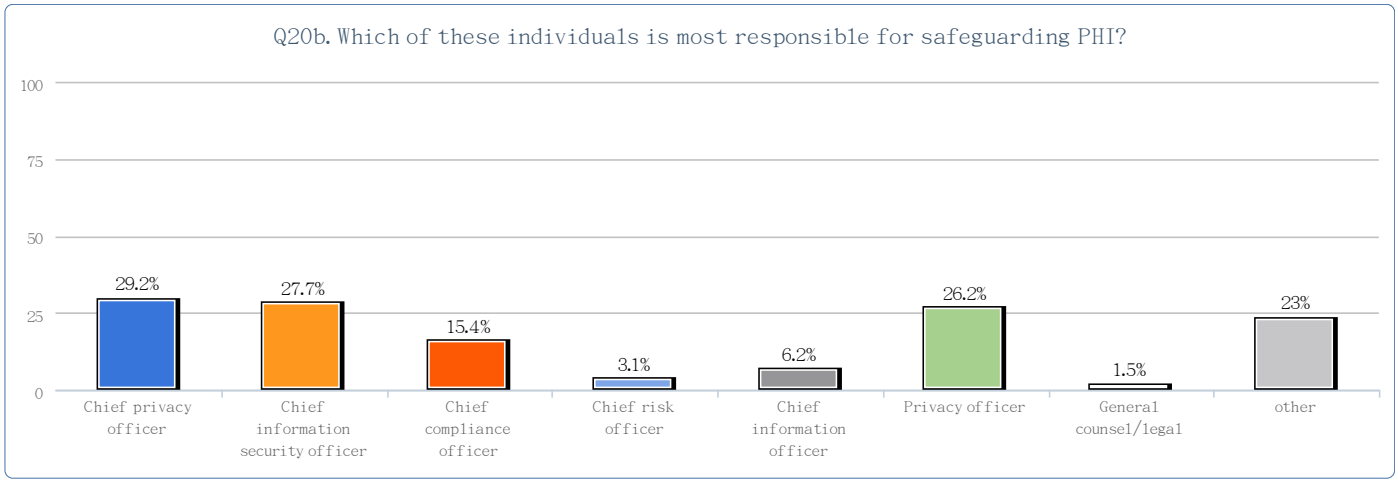
Statistics	
Total Responses	65



Q20a. Who within your organization is responsible for safeguarding PHI? Please check all that apply.

Value	Count	Percent %
Chief privacy officer	27	41.5%
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%

Statistics	
Total Responses	65



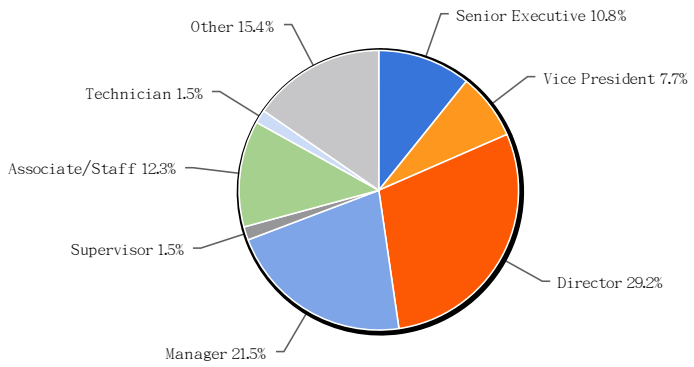
Q20b. Which of these individuals is most responsible for safeguarding PHI?

Value	Count	Percent %
Chief privacy officer	19	29.2%
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%

Statistics	
Total Responses	65

Other (please specify)	8	12.3%
No one person has overall responsibility	6	9.2%

D1. What organizational level best describes your current position?

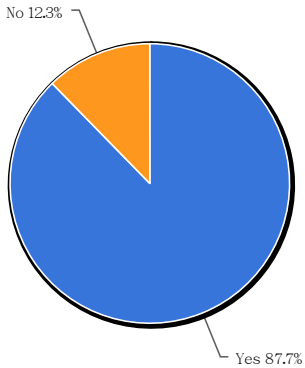


D1. What organizational level best describes your current position?

Value	Count	Percent %
Senior Executive	7	10.8%
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%

Statistics	
Total Responses	65

D2. Is this a full time position?

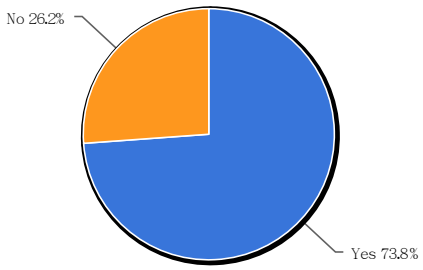


D2. Is this a full time position?

Value	Count	Percent %
Yes	57	87.7%
No	8	12.3%

Statistics	
Total Responses	65

D3. Do you as an individual have direct oversight responsibility within your organization for safeguarding PHI?

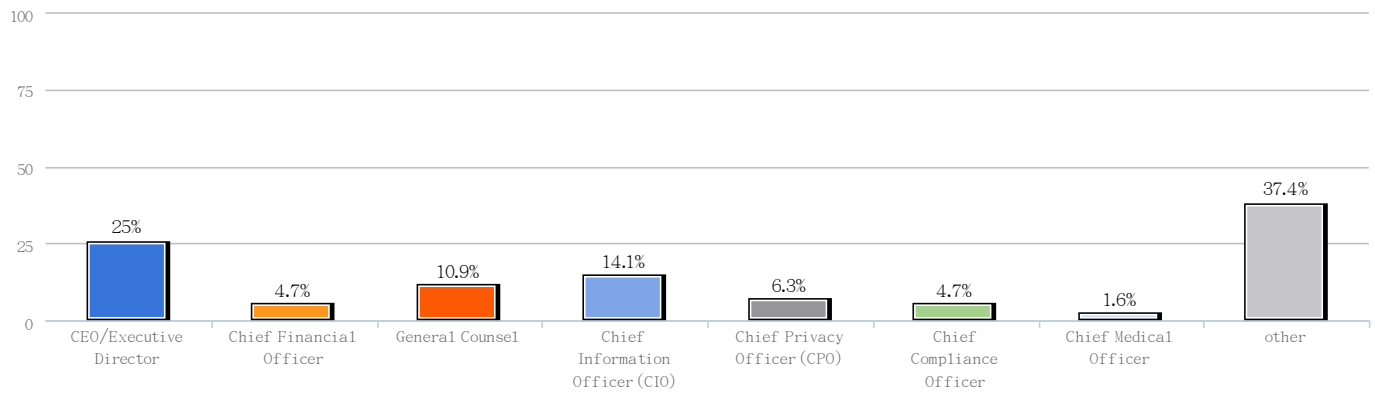


D3. Do you as an individual have direct oversight responsibility within your organization for safeguarding PHI?

Value	Count	Percent %
Yes	48	73.8%
No	17	26.2%

Statistics	
Total Responses	65

D4. Check the Primary Person you report to within the organization.

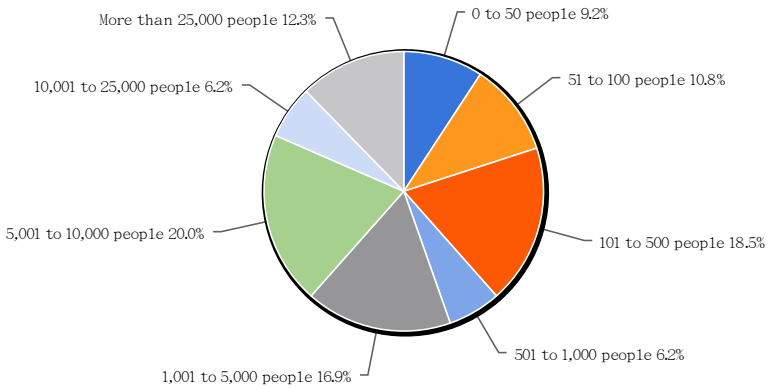


D4. Check the Primary Person you report to within the organization.

Value	Count	Percent %
CEO/Executive Director	16	25%
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%

Statistics	
Total Responses	64

D5. What is the total headcount of your organization?

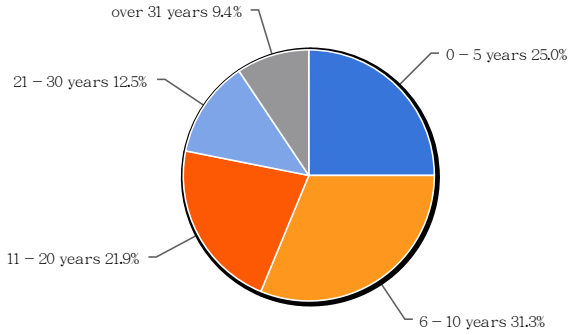


D5. What is the total headcount of your organization?

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

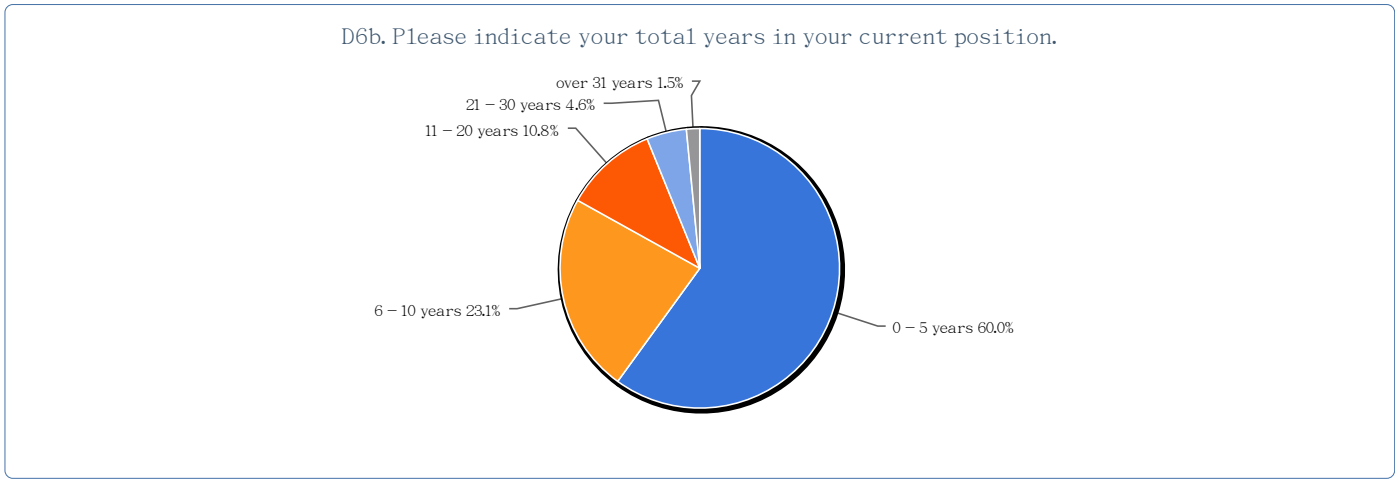
D6a. Please indicate your total years of professional experience related to safeguarding PHI.



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%

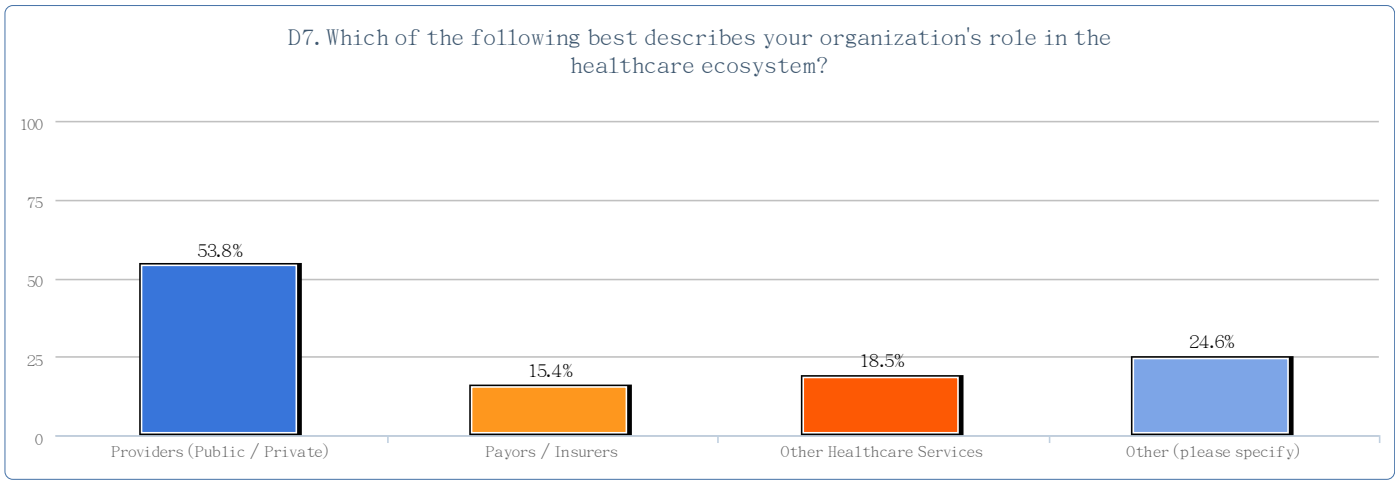
Statistics	
Total Responses	64
Sum	442.0
Average	10.5
StdDev	5.54
Max	21.0



D6b. Please indicate your total years in your current position.

Value	Count	Percent %
0 – 5 years	39	60%
6 – 10 years	15	23.1%
11 – 20 years	7	10.8%
21 – 30 years	3	4.6%
over 31 years	1	1.5%

Statistics	
Total Responses	65
Sum	230.0
Average	9.2
StdDev	4.87
Max	21.0



D7. Which of the following best describes your organization's role in the healthcare ecosystem?

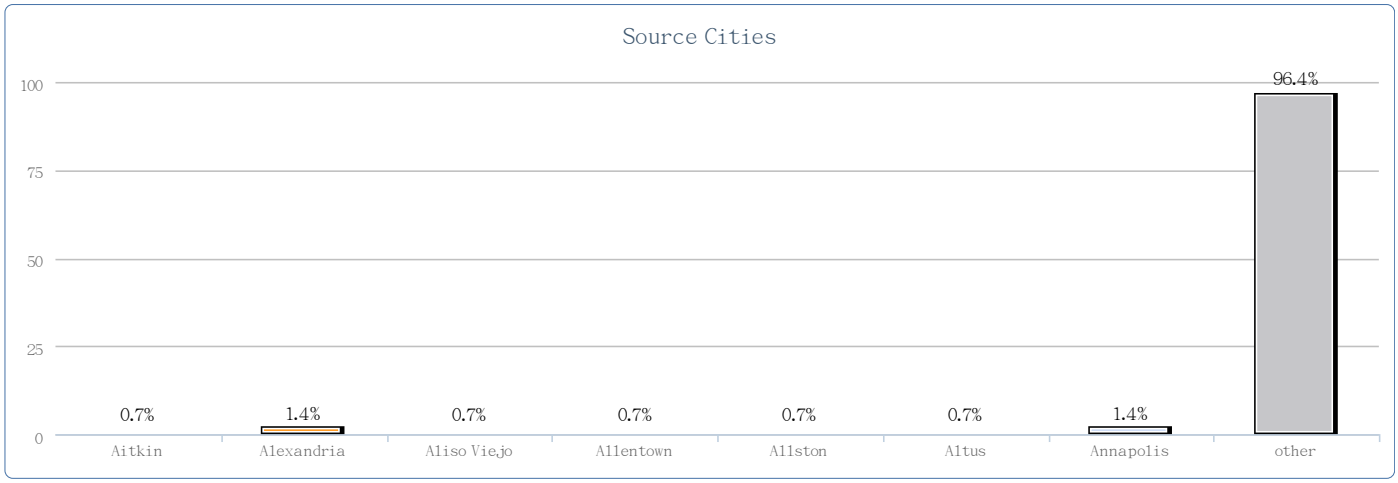
Value	Count	Percent %
Providers (Public / Private)	35	53.8%
Payors / Insurers	10	15.4%
Other Healthcare Services	12	18.5%
Other (please specify)	16	24.6%

Statistics	
Total Responses	65

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.



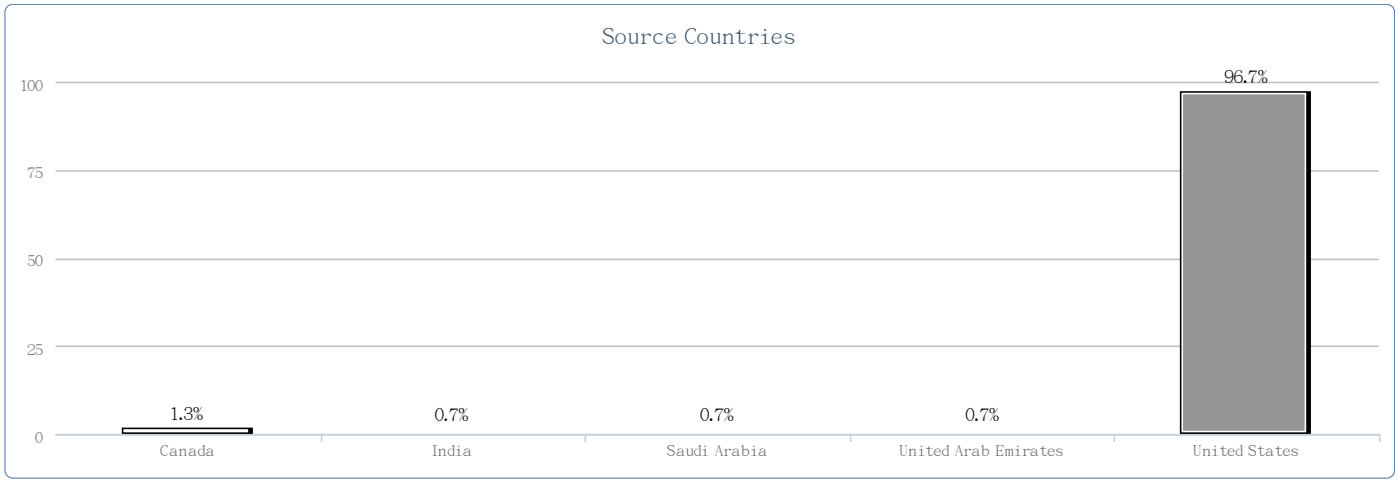
Source Cities

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