The Complete Guide to Healthcare Privacy and Information Security Governance

Phyllis A. Patrick, MBA, FACHE, CHC

Foreword by **Larry Ponemon, Ph.D.**

The Complete Guide to Healthcare Privacy and Information Security Governance

Phyllis A. Patrick, MBA, FACHE, CHC
Foreword by Larry Ponemon, Ph.D.

HCPro
a division of BLR

The Complete Guide to Healthcare Privacy and Information Security Governance is published by HCPro, a division of BLR.

ISBN: 978-1-61569-359-7

Phyllis A. Patrick, MBA, FACHE, CHC, Author
Gerianne Spanek, Managing Editor
Adam Carroll, Copyeditor
Erin Callahan, Senior Director, Product
Melissa Osborn, Product Director, Group Publisher
Vicki McMahan, Sr. Graphic Designer
Tyson Davis, Cover Design
Jason Gregory, Graphic Design/ Layout

Arrangements can be made for quantity discounts. For more information, contact:

HCPro
75 Sylvan Street, Suite A-101
Danvers, MA 01923
Telephone: 800-650-6787 or 781-639-1872
Fax: 800-639-8511
Email: *customerservice@hcpro.com*

Visit HCPro online at *www.hcpro.com* and *www.hcmarketplace.com*

Contents

About the Author

Phyllis A. Patrick, MBA, FACHE, CHC

Phyllis A. Patrick is the founder and president of Phyllis A. Patrick & Associates LLC, a consulting group that provides strategic planning, security, and privacy services to the healthcare industry. Clients include academic medical centers, community hospitals, physician groups, vendors and business associates, health information exchanges, and pharmaceutical companies.

Patrick has held senior positions in privacy, security, and compliance at major academic medical centers in New York City. She was named the first information security officer at Mount Sinai Medical Center in Manhattan. As vice president and chief compliance officer at Hospital for Special Surgery in Manhattan, she created and directed the organization's compliance program, which included its privacy and security programs.

Patrick is a member of the Ponemon Institute's RIM (Responsible Information Management) Council, a select group of privacy, security, and information management leaders from multinational corporations who are privacy, security, and data protection champions within their respective industries. She is a frequent speaker at national and regional conferences and professional associations, including the HIPAA Summit, academic medical center privacy and security conferences, Health Care Financial Management Association, Health Care Compliance Association, and Association of Healthcare Internal Auditors.

A longtime member of the Greater New York Hospital Association, Patrick was a founding member of its security work group and a contributing member of the compliance work group. She is a member of the North Carolina Healthcare Information and Communications Alliance, Inc., privacy and security work group and a member of the New England Healthcare Internal Auditors board of directors. Patrick is a member of the editorial advisory board of *Briefings on HIPAA*, published by HCPro, and a member of the governance, risk, and compliance advisory board for Wolters Kluwer Law & Business.

Patrick received a BS in psychology from Pennsylvania State University and an MBA in healthcare administration from Cornell University. She is a fellow in the American College of Healthcare Executives and is certified in healthcare compliance.

Visit Phyllis A. Patrick & Associates LLC at *http://www.phyllispatrick.com/*. Contact Patrick at *info@phyllispatrick.com.*

About the Contributor

Larry Ponemon, PhD

Larry Ponemon is the chairman and founder of the Ponemon Institute, a research think tank dedicated to advancing privacy, data protection, and security practices. Ponemon is considered a pioneer in privacy auditing and the responsible information management (RIM) framework. *Security Magazine* has named him one of the "Most influential people for security."

Ponemon was appointed to the U.S. Federal Trade Commission Advisory Committee on Online Access and Security, the U.S. Department of Homeland Security Data Privacy and Integrity Advisory Committee, and two California task forces on privacy and security laws. He serves as chairman of the Government Policy Advisory Committee and co-chair of the Internet Task Force for the Council of American Survey Research Organizations (CASRO).

Previously, Ponemon was a senior partner at PricewaterhouseCoopers, where he founded the firm's global compliance risk management group. He also served as the national director of business ethics services at KPMG Peat Marwick and executive director of the KPMG Business Ethics Institute.

Ponemon has presented hundreds of keynote speeches at national and international conferences on privacy, data protection, information security, corporate governance, and RIM. He also has held tenured faculty positions and has written numerous articles and books.

An active member of the International Association of Privacy Professionals, Ponemon also was a founding member of the Certified Information Privacy Professional (CIPP) Advisory Board. He earned his PhD at Union College in Schenectady, N.Y., and attended the doctoral program in system sciences at Carnegie Mellon University in Pittsburgh. He earned a BS with highest distinction from the University of Arizona in Tucson.

Ponemon is a certified public accountant and a certified information privacy professional.

Visit the Ponemon Institute at *www.ponemon.org/*. Contact Ponemon at *research@ponemon.org*.

Foreword

Privacy and information security governance in healthcare organizations has always been a challenge. For several reasons, however, the privacy and security of patient information faces new and expanded threats. Since conducting our first benchmark study on patient privacy and security in 2010[1], criminal attacks on healthcare systems have risen a startling 100%.

Data breach incidents continue to plague healthcare organizations. Our research reveals that some healthcare organizations have experienced data breach incidents that cost millions of dollars. Based on the experience of the healthcare organizations we have studied over the years, we believe the potential cost to the healthcare industry could be as much as $5.6 billion annually.[2]

Our research also shows healthcare employees contribute to data breach risks because of their personal unsecured devices (smartphones, laptop computers, and tablets). In addition, healthcare organizations continue to struggle to comply with increasing complex federal and state privacy and security regulations. Most notable is the impact of the recent Affordable Care Act on the security of patient information.

These factors all point to the necessity of good governance in healthcare organizations. However, establishing an effective privacy and security program that is accountable to patients, the community, clinicians, colleagues, and regulators can be a daunting task.

This is why I am so pleased to recommend *The Complete Guide to Healthcare Privacy and Information Security Governance* to every professional responsible for overseeing privacy and information security programs in healthcare organizations. What sets this book apart from others is its focus on the role of the board of directors and how critical its oversight responsibilities are to the management of these programs.

The Complete Guide to Healthcare Privacy and Information Security Governance provides practical guidance on every aspect of healthcare governance. For example, it describes how to conduct a

1 Fourth Annual Benchmark Study on Patient Privacy & Data Security, conducted by Ponemon Institute and sponsored by IDExperts, March 2014

2 This is based on multiplying $986,948 (50% of the average two year cost of a data breach experienced by the 91 healthcare organizations in this research) x 5,723 (the total number of registered U.S. hospitals, according to the American Hospital Association).

comprehensive risk assessment and presents a detailed methodology for evaluating privacy and information security programs.

I also believe that what makes this book such an indispensable and valuable resource is its recognition that the management of these programs requires many functions to collaborate to ensure successful outcomes. It should be read and frequently referenced by clinicians, healthcare managers and informatics officers, as well as those in compliance, internal audit, legal services, and human resources management, and many others.

Larry Ponemon, PhD
Chairman and Founder
Ponemon Institute

Introduction

This book aims to dispel the notion that the Health Insurance Portability and Accountability Act (HIPAA) is the raison d'être for privacy and information security programs.

Health information represents the most sensitive data regarding individuals and groups of people. As a result of healthcare reform, changing technologies, and increasing use of electronic health records, patients are becoming more directly involved in their care. This includes managing their individual health information. Patients want to be certain that health information is as secure and accurate as their financial and academic records and other aspects of their lives that are digitized.

Maintaining the privacy of individuals' health information is the responsibility of all healthcare providers, researchers, insurance companies, health information exchanges, and other entities that use this information for a variety of purposes beyond the physician-patient relationship. Leaders and workforce members at all levels of healthcare organizations and entities that perform work on behalf of healthcare entities are responsible for ensuring the privacy and security of information assets.

HIPAA requirements represent the tip of the proverbial iceberg. U.S. Department of Health and Human Services Office for Civil Rights regulators describe it as the "floor" with respect to what is required of healthcare organizations to protect patient data and related information assets. A host of other state and federal privacy and security requirements apply to healthcare organizations. This trend will intensify as healthcare organizations merge, affiliate, consolidate, and develop new models of care and sustainable business models, such as accountable care organizations and medical homes.

Healthcare organizations are also subject to the Payment Card Industry Data Security Standard (PCI DSS), the Clinical Laboratory Improvement Amendments (CLIA), the Patient Safety and Quality Improvement Act (PSQIA), the Children's Online Privacy Protection Rule (COPPA), the Fair and Accurate Credit Transaction Act (FACTA), Food and Drug Administration (FDA) rules, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and laws that govern electronic media and protect information assets. Various state laws that address breach notification, protection of personal information, encryption, and medical records also affect healthcare organization's privacy and information security programs.

As use of electronic media in healthcare organizations increases, so too will laws that govern their use. Increasing demand and the expectations of clinicians, patients, and researchers to control

individual health information while meeting the challenges of improving the health of individuals and populations will require new and innovative approaches to protecting privacy. This book provides essential information and an expert perspective on developing and implementing effective privacy and information security programs that are accountable to patients, the community, clinicians, colleagues, and regulators. The book is designed for privacy and information security professionals who are responsible for management and day-to-day operations of these programs. This includes planning, measurement, and reporting activities.

The interdisciplinary nature of healthcare processes and the consolidation of many functions across organizations also makes this book useful for clinicians and healthcare managers, including compliance officers, internal auditors, informatics officers, legal services staff, safety officers, quality officers, procurement officers, health information management professionals, information technology professionals, risk managers, researchers, educators, human resources management, and others responsible for safeguarding information assets and working with privacy and information security officers.

Finally, the book also provides important information for senior leaders and trustees with respect to their role in and responsibility for overseeing privacy and information security programs.

The book includes seven chapters and an online Appendix of resource materials and references for professionals and others interested in privacy and information security. Each chapter concludes with questions that privacy and information security professionals and other stakeholders can use for review, discussion, and program evaluation.

Chapter 1 provides an introduction to privacy and information security, including basic concepts, privacy impact analysis and medical identity theft, organization mission and culture, the notice of privacy practices, trends that affect privacy and information security programs, and the effects and consequences of technology.

Chapter 2 describes the evolution of privacy and information security programs from regulation to culture. It includes a historical overview that describes the origin of privacy and information security laws and explains why these programs are more important than ever.

Chapter 3 focuses on risk analysis and risk management, along with principles and practices that form the foundation of effective privacy and information security programs. The chapter addresses HIPAA Security Rule risk analysis requirements and the meaningful use program. It explains the importance of developing a risk profile and evaluating risks to confidential information. It addresses privacy and information security in the context of organizational risk, as well as risk management strategies.

Chapter 4 offers a paradigm involving privacy, security, quality, and safety. Privacy and information security programs are still in the developmental stage, several years behind quality and safety as core cultural values and embedded programs in healthcare. However, the programs' foundations are similar.

Chapter 5 describes the governance aspects and requirements of effective privacy and information security programs, including oversight responsibilities of the board of directors. It explains how to evaluate programs and select privacy and information security models as foundations for the programs.

Chapter 6 provides a 10-point methodology for evaluating privacy and information security programs. It describes key components, including governance, policies and procedures, risk analysis and risk management processes, program infrastructure and resources, education and training programs, physical security, technical security, breach notification policy and procedures, effects of business associate relationships, auditing, and monitoring processes.

Chapter 7 discusses the future of privacy and information security programs in healthcare. It addresses trends affecting the programs and the implications for healthcare organizations, governance issues, the concept of data and information governance, expectations for and skills needed by privacy and information security professionals, the coming transition to information protection and optimization, and governance structures and processes of the future.

1

Introduction to Privacy and Information Security

Information privacy and security, key aspects of privacy in general, affect our lives in many ways—through our relationships with retailers, banking and financial institutions, and insurance companies; our purchasing decisions; our health status. These topics as they relate to healthcare feature prominently in our personal and online conversations, and news media outlets present information daily.

Privacy is an ethical issue. It involves the rights of individuals with respect to the use and distribution of their personal and private information, as well as the consent individuals give regarding that information's use and disclosure. Key questions arise from this concept. Does a patient have the right to verify any personal and health information held by a provider, and if so, can the patient correct or amend that information? Does the patient have the right to know who is using his or her medical information and for what purposes?

Despite the pervasiveness of healthcare information and communications, privacy and information security are not well understood by many healthcare managers and providers. Achieving and sustaining privacy for patients in the medical world involves understanding complex relationships and processes. Uses and disclosures of health information are at the core of patient care delivery, care coordination, safety, healthcare financing, research, education, and other aspects of the healthcare delivery system.

Program Basics: Protecting Patient Privacy

Healthcare involves a partnership between patients, clinicians, and other professionals. Open communication, respect for personal and professional standards, and understanding how parties differ help ensure that patients receive the best possible care.

Physicians and other healthcare practitioners have always had a duty to maintain patients' confidences. This duty means that providers may not disclose any medical information that patients reveal to them or that they discover during treatment. When patients know providers will protect the

confidentiality of their health information, they are enabled to make a complete and frank disclosure of that information. This full disclosure, in turn, allows clinicians to diagnose conditions properly and treat patients appropriately.

The U.S. Department of Health and Human Services (HHS) has invested billions of dollars in the development and expansion of electronic health records (EHR). Building confidence in the security of EHRs and strengthening patients' rights with respect to use and access to their records were key driving forces for the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule provisions. The HHS Office for Civil Rights (OCR), which oversees compliance with HIPAA rules, has provided a foundation for a new era of security and privacy in healthcare.

Healthcare organizations typically include provisions in their Patients' Bill of Rights that aim to protect the confidentiality of individual patient information. Organizations also develop codes of conduct that describe how workforce members are expected to conduct themselves, including guidelines and rules for protecting the confidentiality of patient information.

The American Hospital Association (AHA) developed *A Patient's Bill of Rights* in 1973 and modified it in 1992. The goal of this bill was to improve the effectiveness of patient care. In 2003, to emphasize the patient-provider relationship, the AHA replaced the *Bill of Rights* with *The Patient Care Partnership*, which states:

> *We respect the confidentiality of your relationship with your doctor and other caregivers, and the sensitive information about your health and health care that are part of that relationship. State and federal laws and hospital operating policies protect the privacy of your medical information. You will receive a Notice of Privacy Practices that describes the ways that we use, disclose and safeguard patient information and that explains how you can obtain a copy of information from our records about your care.*[1]

Many healthcare organizations have adopted the AHA model bill and *The Patient Care Partnership* for use and distribution to their patients.

The American Medical Association developed *Fundamental Elements of the Patient-Physician Relationship* in 1990. Its core theme is collaboration between patient and caregiver with an emphasis on patients' personal responsibility for their health.[2] *Fundamental Elements of the Patient-Physician Relationship* states:

> *The patient has the right to receive information from physicians and to discuss the benefits, risks, and costs of appropriate treatment alternatives. Patients should receive guidance from their physicians as to the optimal course of action. Patients are also entitled to obtain copies or summaries of their medical records, to have their questions answered, to be advised of potential*

1 American Hospital Association. The Patient Care Partnership, 2003. *www.aha.org/advocacy-issues/communicatingpts/pt-care-partnership.shtml*

2 American Medical Association. Fundamental Elements of the Patient-Physician Relationship, 1990. *www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion1001.page*

conflicts of interest that their physician might have, and to receive independent professional opinions ….

The patient has the right to confidentiality. The physician should not reveal confidential communication or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest.[3]

The HIPAA Rules

The HIPAA Omnibus Rule, which became effective in 2013, represents the most significant changes to HIPAA since the original act became law in 1996. It emphasizes patient rights and patient empowerment through provisions addressing protected health information (PHI) and how patients can access, control, use, and disclose their PHI.

The Omnibus Rule includes changes to the Privacy Rule, with an emphasis on providing more rights to patients regarding access to and control of their PHI. The Omnibus Rule implements most of the privacy and security provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act. It adopts enforcement penalties in place since 2009 and revises the Breach Notification Rule to state that a breach incident is presumed to have caused harm unless a risk analysis is conducted to demonstrate otherwise. Lastly, the Omnibus Rule also includes a final Enforcement Rule.

The Security Rule has not changed. However, the Omnibus Rule extends the provisions of the Security Rule to business associates (BA) and subcontractors. Covered entities (CE) now must understand the security practices of their BAs and subcontractors, and they must consider assessing how BAs are working to achieve effective breach notification and mitigation processes.

The basic tenets of the four rules included in the HIPAA Omnibus Rule are as follows.

The HIPAA Privacy Rule, effective since 2003, addresses the use and disclosure of PHI by organizations subject to the Privacy Rule.

The intent of the Privacy Rule is ensuring that PHI is protected during the flow of information that is necessary to provide and promote high-quality care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information, while protecting the privacy of individuals who seek healthcare. It prescribes permitted and required uses and disclosures of information for treatment, payment, and healthcare operations.

A central component of the Privacy Rule is the "minimum necessary" principle that governs use and disclosure of PHI.

A CE must develop, distribute, and make available a Notice of Privacy Practices (NPP) that describes how it may use and disclose PHI.

3 Ibid.

The Privacy Rule requires the development and implementation of privacy policies and procedures, designation of a privacy official responsible for the program, designation of an individual responsible for receiving complaints and providing information, workforce training and management, documentation and record retention, and other administrative requirements.

The Breach Notification Rule requires that CEs notify individuals and the secretary of HHS of any breach of unsecured PHI that has occurred or which they reasonably believe has occurred. Unsecured PHI refers to PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the HHS secretary.

The notification to HHS must occur no later than 60 days after discovery of the breach. If the breach involves more than 500 individuals, local news outlets must also be notified. Breaches affecting fewer than 500 individuals must be reported annually, within 60 days following the end of the preceding calendar year.

CEs must maintain logs of all data security breaches and documentation of investigations and risk analyses. Breach reporting is not required if the data involved is rendered unreadable via encryption. PHI that is encrypted or disposed of securely is considered to have met "safe harbor" provisions.

BAs must notify their CEs when a breach occurs on their watch. The CE is responsible for notifying the individuals whose PHI has been breached. Companies that sell personal health records must comply with a similar U.S. Federal Trade Commission breach notification rule. If a subcontractor of a BA experiences a breach, it must notify the BA, which in turn notifies the CE.

The Security Rule, enforceable since April 2005, applies to PHI that a CE receives, creates, maintains, or transmits in electronic form. The Security Rule includes administrative, physical, and technical safeguards to protect electronic PHI (ePHI).

Examples of safeguards include the following:

- Administrative safeguards—Risk analysis, security incident procedures, access controls, disaster recovery planning, security awareness training for all workforce members
- Physical safeguards—Workstation security, policies and procedures to address the storage and disposal of ePHI
- Technical safeguards—Unique user authentication, audit controls, data integrity, encryption

Security Rule standards are based on the following concepts:

- Flexibility and scalability—A security program should be based on an organization's size, complexity, and capabilities
- Comprehensive in scope—The program should address all aspects of security (i.e., behavioral and technical)
- Technology neutral—The program's standards should remain constant as technology changes

A breach of confidentiality occurs when confidential patient information, obtained through the patient-physician relationship, is disclosed to a third party absent patient consent or court order. Such a disclosure may be oral, written, or electronic. It can occur by telephone, fax, email, or health information exchange or network.

Specifically, breach is "the acquisition, access, use, or disclosure of protected health information in a manner not permitted … which compromises the security or privacy of the protected health information."[4] The term "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 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 … (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 healthcare 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 … (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."[5]

Further, "impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised."[6]

Various federal and state laws protect medical records and sensitive patient information (e.g., HIV status, genetic testing or screening information, mental health records, drug and alcohol abuse records, and rehabilitation information). In addition, patients have a basic expectation that physicians and other providers will respect their privacy. As such, any breach in confidentiality, even if it appears to be minor, can lead to patient mistrust, erosion of the patient-physician relationship, and possible legal action by patients and/or state attorneys general.

OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules. Its ongoing compliance and audit program includes investigations of complaints and random audits of CEs and BAs. The HIPAA Enforcement Rule prescribes the penalties, fines, corrective action plans, and monitoring procedures that OCR uses to enforce HIPAA.

Refer to "Policy Roadmap: Meeting Omnibus Rule Requirements" in the online Appendix. CEs and BAs can use it to review and revise privacy, security, and breach notification policies. It includes relevant Privacy, Security, and Breach Notification Rule citations, along with key changes and additions required by the HIPAA Omnibus Rule and affected departments and functions.

4 45 CFR 164.402.

5 Ibid.

6 Ibid.

The changes under the Omnibus Rule require collaboration by many departments and individuals. An example is the right of a patient who pays for service out of pocket to restrict or prevent the disclosure of medical information generated from this encounter to the individual's health plan. The Policy Roadmap illustrates that policies and procedures not within the purview of privacy and information security officers may require revision. Examples include health information management, fundraising and development, registration, admitting, and patient access. Think of privacy and information security as a team sport, with various management areas responsible for different components of an organization's program.

HIPAA rules give an organization's privacy and information security officers plenty to do. Many programs focus on HIPAA requirements through policies, training, and investigative processes. However, HIPAA represents the "floor" of privacy and information security requirements and practices for healthcare and other entities. State privacy and information security requirements are also important and must be considered when developing policies and procedures. Notably, state laws pertaining to many aspects of privacy and information security, including protection of medical records, reporting of breaches, and prevention of identity theft, are often more complex and rigorous than HIPAA. Other federal laws also apply to healthcare enterprises. Refer to Chapter 2 for additional information.

Protected Health Information Concepts

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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 healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.[7]

The information identifies the individual or there is reasonable basis to believe that the information can be used to identify the individual. Individually identifiable health information includes many common identifiers.

PHI refers to any information in a patient's medical record or designated record set that can be used to identify that patient. It is information that was created, used, or disclosed in the course of providing a healthcare service such as diagnosis or treatment. If all identifiers are removed or encrypted, information becomes de-identified or anonymized and is no longer considered PHI. (Refer to Figure 1.1 for a list of PHI identifiers.)

7 45 CFR 160.103.

Figure 1.1

Protected Health Information Identifiers

Name.

All geographical subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes. (Exceptions: The first three digits of a ZIP code if the geographic unit formed by combining all ZIP codes with the same three initial digits contains fewer than 20,000 people and the initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000.)

All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death; and all ages over 89 and all elements of dates (including year) indicative of such age (except that such ages and elements may be aggregated into a single category of age 90 or older).

Telephone numbers.

Fax numbers.

Electronic mail addresses.

Social Security numbers.

Medical record numbers.

Health plan beneficiary numbers.

Account numbers.

Certificate/license numbers.

Vehicle identifiers and serial numbers, including license plate numbers.

Device identifiers and serial numbers.

Web universal resource locators (URL).

Internet protocol (IP) address numbers.

Biometric identifiers, including fingerprints and voiceprints.

Full-face photographic images and any comparable images.

Any other unique identifying number, characteristic, or code (except a random identifier code for the subject that is not related to or derived from any existing identifier).

There are also standards and criteria to protect an individual's privacy from re-identification. Any code used to replace the identifiers in data sets may not be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed.

HIPAA allows researchers to access and use PHI when necessary. Researchers must not have actual knowledge that would enable re-identification of the research subject with remaining PHI identifiers used in the study.

PHI is an important asset for healthcare organizations and their BAs. It enables healthcare providers to fulfill their patient care, research, and education missions. PHI is everywhere; creation of databases and increasing use of analytics has expanded the volume of data both within and outside organizations. Proliferation of EHR technology and the growing use of data in research settings has magnified the importance of safeguarding PHI.

Privacy Impact Analysis

Healthcare organizations must assess the privacy impact of new projects and changes in processes because they may affect the receipt, use, maintenance, or transmission of patient information. Assessing privacy impacts is essential for understanding how information flows through an organization and how to develop safeguards to protect the information.

Most organizations have not taken the time to describe and document their flow of information and how it will be used in new projects and processes; if they have, that documentation may not be current. Despite efforts during the early 2000s upon implementation of the HIPAA Privacy and Security Rules, privacy impact analyses have not kept pace with changes in healthcare information technology (IT), other regulatory requirements (e.g., identity theft prevention, state privacy laws), and delivery process changes (e.g., medical homes and accountable care organizations).

Ongoing privacy impact analyses facilitate understanding and documentation of the possible effects on patient privacy as an organization changes its programs and processes, implements new trends in technology, and develops new services.

Medical identity theft

Medical identity theft occurs when an individual commits fraud by acquiring and using another individual's name and other portions of his or her identity (e.g., Social Security number, demographic information, health insurance number) without that individual's knowledge or consent. The individual committing fraud may be able to use the other person's information to obtain medical services or devices, acquire prescription medications, make false claims for medical services, or receive insurance reimbursements.

Medical identity theft leads to incorrect and fraudulent entries into its victims' medical records. These revised medical records do not accurately describe their specific health conditions, medications, and other relevant healthcare information, resulting in risk of harm to the defrauded patients and potentially compromising quality of care. Victims may be billed for services they did not receive, have their credit scores impacted, lose medical insurance, and undergo other complex and daunting financial stressors. Medical identity theft is very difficult to address after fraud has occurred because victims have limited rights and methods to resolve it.

The incidence of medical identity theft has increased over the years. "An estimated 1.49 million Americans were affected by medical identity theft in 2011 for a national impact of $30.9 billion."[8] Healthcare-related identity theft accounted for 43% of all identity thefts reported nationally in 2013, according to a report by the Identity Theft Resource Center.[9] This represents a larger share than identity theft involving banking and finance, government, military, or education.[10]

Researchers completing the 2013 *Survey on Medical Identity Theft,* conducted by the Ponemon Institute, found that medical identity theft continues to be a costly and potentially life-threatening crime. This study of more than 700 victims of medical identity theft found that, unlike other forms of identity theft, the medical identity thief is most likely someone the victim knows. Most cases of identity theft result not from data breaches, but from sharing personal identification and medical insurance credentials with family members and friends. Also, family members sometimes take victims' credentials without permission.[11]

Analyzing the effect of medical identity theft on privacy will help healthcare organizations develop new processes and amend existing processes to protect the authenticity and integrity of individuals' medical records and to prevent patients from being billed for services they did not receive. For example, many hospitals stopped using Social Security numbers on admission face sheets and other documents several years ago to reduce the opportunities for compromise of this key identifier. Admissions processes were not adversely affected by this change, and patient relations improved when patients understood that hospitals were trying to protect their privacy.

Changes pertaining to policies, processes, and procedures minimize patient risk without compromising care provision and coordination. Privacy assessments help healthcare organizations identify what changes to make.

Mission and Culture: Privacy and Information Security

Hospitals and healthcare organizations devote much time and attention to crafting mission statements. These statements are prominently posted, included on websites, and inserted into various documents provided to patients, community members, and others. Mission statements generally emphasize organizations' service areas and include information about providing care to enhance community health, maintaining financial sustainability, working with others, providing high-quality services, and emphasizing a safe environment. They may also address education and research at teaching and academic institutions. However, mission statements rarely address confidentiality—an omission that speaks loudly.

8 Ponemon Institute. Second Annual Survey on Medical Identity Theft, 2011. *https://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/1_types%20of%20fraud_medical%20study.pdf*

9 Kaiser Health News, February 7, 2014.

10 Identity Theft Resource Center. 2013 Data Breach Category Summary. *http://www.idtheftcenter.org/images/breach/UPDATED_ITRC_Breach_Stats_Report_Summary_2013.pdf*

11 Medical Identity Fraud Alliance. Ponemon Institute 2013 Survey on Medical Identity Theft. *http://medidfraud.org/2013-survey-on-medical-identity-theft/*

When healthcare executives and boards of directors think of privacy and information security, HIPAA rules, breaches, compliance, and IT generally come to mind first. Most healthcare organizations understand the risks of a security breach, including loss of reputation and patient/community trust, possible fines, reporting requirements, and diversion of financial resources to investigate and remediate harm.

Yet despite the publicity about the number and types of breaches occurring in healthcare, and enforcement of the Breach Notification Rule, protection of patient information has not improved in many organizations. A Ponemon Institute survey found that 45% of respondents said their organizations (including hospitals and clinicians) had not experienced a change in effectiveness in protecting patient information, and 30% said their programs had become less effective. The majority of respondents had also experienced a cyber attack or intrusion of their IT infrastructure in the previous 24 months.[12]

The question is not if a breach will occur, but when. Patient information threats and vulnerabilities, whether in electronic systems or on paper, are constantly changing. Thus, a dynamic, formal, ongoing privacy and information security program is vital to reducing both threats and any actual patient harm. Security is not a onetime process; it must be continuous.

The HIPAA Security Rule and other security regulations and models require organizations to develop incident response plans. The Breach Notification Rule requires organizations to develop breach investigation and mitigation processes. All these efforts must be internalized and integrated into an organization's culture to be most effective. They must be integral to and include ongoing privacy and information security risk assessment and management.

In most healthcare organizations, sadly, this does not happen. Privacy and information security are seen as regulatory requirements, often associated with compliance and/or IT activities. Few organizations approach privacy and information security with the same scope of work as safety and quality programs, nor do they attach the same amount of importance to a security program as they would a safety or quality program. Simply put, privacy and information security are not embedded in organizations' missions or their workforce's cultural expectations.

The Ponemon survey assessed barriers to achieving a strong IT security posture (i.e., developing reactive programs). More than half of respondents (54%) said that "leadership lacks commitment to achieving a strong security posture," and 33% reported a "lack of oversight or governance" associated with security programs. Nearly one-third of respondents (31%) reported that "security resources and/or budget are inadequate." Failure to conduct security risk assessments as often as they should occur and lack of ongoing security education and training were reported by 16% and 10% of respondents, respectively.[13]

The Ponemon survey further revealed that 37% of respondents could not determine the proportion of IT security spending relative to the total IT budget allocated to security, and 27% could not determine

12 Ponemon Institute. The Economic and Productivity Impact of IT Security on Healthcare, May 2013, p. 14.

13 Ibid., p. 10.

the percentage of IT spending dedicated to patient engagement (e.g., patient portals, secure messaging, and other forms of electronic communication). More than one-fourth of respondents (26%) reported that their organizations spend 11%–15% of their IT budgets on patient engagement initiatives, and 12% reported that their organizations spend 11%–15% on IT security spending.[14]

These results and the results of other surveys (e.g., annual surveys of IT leadership conducted by the Health Information Management Systems Society, a national organization of IT professionals) indicate that healthcare organizations are not approaching privacy and information security as seriously as they should.

With the evolution of healthcare reform and government priorities for health information exchange, the proliferation of data of all types, changing consumer and patient expectations, technology advances, and regulatory requirements for safeguarding information, healthcare organizations face increasing challenges in achieving their missions and meeting their commitments to patients and the community.

Board members and senior leaders must face these challenges and provide oversight of privacy and information security programs. In turn, privacy and information security officers must communicate more effectively about their programs. This includes using meaningful metrics and soliciting support and collaboration from managers across the organization. Officers require the support of senior leaders to develop and strengthen their programs. Leaders, meanwhile, need solid understanding and knowledge of the components of effective privacy and information security programs and what these programs mean to their organizations. Discussions related to safety, quality, data governance, risk assessment, and risk management should address privacy and information security.

Privacy and information security officer job descriptions should clearly state the responsibilities and accountabilities of these positions. Oversight responsibilities of trustees and senior leaders should be clearly delineated as part of their fiduciary responsibilities, including privacy and information security in committee charters and ongoing board training. Goals for the board of directors and senior leadership should include developing knowledge leaders in privacy and information security to guide their organizations in the development and ongoing enhancements of these programs.

Notice of Privacy Practices: A Contract With Patients and the Community

Healthcare organizations are accountable, first and foremost, to the patients they serve and their communities. HIPAA requires CEs to provide every patient an NPP that describes how their PHI may be used and disclosed, patients' rights and responsibilities with respect to their PHI, and the responsibilities of the healthcare provider with respect to PHI it creates, uses, receives, and maintains.

The NPP is one of the most misunderstood documents in healthcare organizations. Though it has been a requirement since the Privacy Rule became effective in 2003, many healthcare organizations view its posting and distribution simply as a rote regulatory process. Few individuals understand its intent

14 Ibid., pp. 21, 23.

or importance, and responses to the question, "When did you last read your organization's NPP?" are usually dismal.

The NPP is essentially an organization's contract with its patients. CEs are required to develop and distribute NPPs that provide a clear and accurate explanation of the rights and practices established in the Privacy Rule. The intent of an NPP is to focus individuals on privacy issues and concerns, prompt discussions with their providers and health plans, and encourage them to exercise their rights.[15]

NPPs can take many forms: a booklet, a layered notice with summary information followed by the full notice, a full-page presentation with graphical elements, or a text-only notice. However it's presented, an NPP must be written in clear and plain language and must describe the following:

- How the CE may use and disclose PHI
- Individuals' rights with respect to their information and how to exercise these rights, including how to register a complaint with the CE
- The CE's legal duties with respect to the information, including a statement that the CE is required by law to maintain the privacy of PHI
- Contact information for requesting additional information about the CE's privacy policies

The HIPAA Omnibus Rule affects the content of NPPs.[16] Effective September 2013, NPPs must include information related to changes in the Privacy Rule, as reflected in organization policies, with a focus on patients' rights to control and access their PHI.

NPPs must include statements that set forth the following:

- Authorization for use and disclosure of psychotherapy notes maintained by the CE is necessary for marketing and the sale of PHI
- Uses and disclosures not described in the NPP will be made only with the individual's written authorization
- Individuals may revoke authorization
- The intent to use PHI for fundraising
- The intent to contact individuals for fundraising
- Individuals may opt out of fundraising communications
- PHI will not be sold without the individual's authorization
- Individuals who pay in full and out of pocket for services may restrict disclosure of PHI to health plans

15 Office for Civil Rights. Notice of Privacy Practices for Protected Health Information (45 CFR 164.520), April 2003.

16 45 CFR 164.520.

- Individuals have the right to be notified after a breach of unsecured PHI

HHS has published model NPPs on its website, with the intent that healthcare providers and health plans can use them to develop and distribute notices that provide clear, approachable, user-friendly explanations of patients' rights with respect to their PHI and the organization's privacy practices. In addition, "[T]he models highlight the new patient right to access their electronic information held in an electronic health record, if their provider has an EHR in their practice."[17]

HIPAA Myths and Misconceptions

Although numerous privacy and security laws apply to healthcare entities, HIPAA rules and requirements tend to receive the most emphasis—and generate the most angst. The terms *HIPAA-compliant vendor, HIPAA cop,* and *HIPAA disciplinary action* are anathema to experienced and serious privacy and information security professionals. HIPAA, as has been noted, represents the floor of requirements intended to protect the privacy and security of patient information. More stringent privacy requirements have existed at the state and national levels for several years before the HIPAA Privacy Rule was implemented (e.g., state medical records laws and requirements). Notably, many organizations implement policies and procedures that are more stringent than that required by HIPAA. Some of this is due to misinformation or misunderstanding of the HIPAA rules.

Greater focus on privacy and information security as key concepts embedded in patient care and organizational culture and a methodical approach to program development could make the process more logical and perhaps less onerous. Consider deleting the term *HIPAA* from policies and processes to the extent possible because this is not where an organization's emphasis should lie.

Various myths and misconceptions surround HIPAA. Examples of HIPAA myth and reality include the following.

Myth: Security is an IT function.

Security involves safeguarding electronic information in various ways and by various means, including policies, processes, education, designation of security officers and managers, dedicating staff and monetary resources to providing technical tools and physical safeguards to protect systems. The Security Rule includes only two standards related to technical security—access controls and audit controls. Most Security Rule standards address administrative safeguards. The rule also includes several physical safeguard and documentation requirements.

IT professionals generally do not receive information security training. Information security is a distinct profession with specific bodies of knowledge and content that address all aspects of protecting an organization's information assets. Many information security officers (ISO) do not report to IT. A conflict of interest may exist if an ISO reports to a chief information officer or other individual in an IT department.

17 U.S. Department of Health and Human Services. Health Information Privacy. *www.hhs.gov/ocr/privacy/hipaa/modelnotices.html*

Security and IT budgets should be separate. This requires an ISO to develop a security budget, justify proposed expenditures, and develop and communicate metrics to demonstrate the program's success and activities.

Myth: Privacy is a subset of compliance.

Although responsibility for privacy is often delegated to compliance officers in healthcare organizations, privacy and compliance are not necessarily compatible functions. They represent separate and distinct bodies of knowledge, with different requirements, regulations, best practices, and approaches. The skill sets for privacy officers and compliance officers are not similar; investigating privacy incidents and security breaches, in collaboration with an ISO, differs from investigating a possible compliance lapse (e.g., a billing problem that raises compliance concerns).

Myth: Governance principles do not apply because privacy and security are subject to regulatory requirements.

Organizations often fail to address privacy and information security in their governance structures and requirements, and this is shortsighted. This practice is changing as leaders realize that privacy and information security involve more than simply complying with regulations. An effective privacy and information security program requires inclusion of governance as a key enabling factor and senior leadership that sets the tone for the program.

Myth: HIPAA is about enforcement, fines, investigations, and finding breaches.

HIPAA enforcement has been increasing since 2009 when OCR was empowered to oversee enforcement of the Privacy and Security Rules in 2003 and 2009, respectively. OCR also provides guidance, educational materials, and technical assistance in developing effective privacy and security programs. Much attention, including media coverage, has focused on investigations and enforcement actions. This, however, should not distract organizations from the true purposes of creating effective programs, providing patients access to their information, and developing health information exchanges to improve quality of care, care coordination, and patient engagement.

Effective training increases awareness of the real purpose of privacy and information security programs. Much of the negativity associated with HIPAA is dispelled when privacy and information security are key components of an organization's culture. Privacy and information security and privacy officers must be empowered to do their jobs and must have resources to develop effective programs. Managers must undergo training to ensure they understand their important roles and responsibilities with respect to privacy and information security program effectiveness. This includes setting workforce expectations. Managers and workforce members are expected to meet organizational safety and quality goals, such as through personnel evaluations and performance improvement plans. Privacy and information security should also be included.

Myth: Focusing on limiting the use of devices that include ePHI and establishing restrictive policies will lead to fewer breaches and possible harm to patient information.

Security is not about restriction and limitation. Instead of erecting barriers to the use of technology, the emphasis should be on employing proven technologies (e.g., secure mobile technology, secure messaging) to ensure that patient care functions can be completed in a timely, safe manner.

Addressing security when planning and designing systems will eliminate the need for restrictive policies, and will remove the need for retrofits and additions after system implementation. Hard-wiring security into the system development life cycle and related processes will ensure that safe practices are followed.

Myth: HIPAA compliance is expensive and diverts resources from other important functions.

A majority (51%) of Ponemon survey respondents think HIPAA security and privacy regulations make delivering quality care more difficult. Most respondents (85%) said HIPAA reduces time available for patient care because of compliance tasks. However, those compliance tasks were not identified, and there is no direct correlation between the regulations and reduction in available time. Thus, this response is likely due to a lack of information and awareness of how security can enhance, not compromise, time spent with patients. Further, 79% of respondents claimed regulations complicate access to electronic information. This is simply not true. Secure biometrics, single sign-on technology, and proximity badges, *when implemented properly*, do not make access to electronic information more difficult. Consider, though, that many organizations still employ user logins and passwords and have many disparate systems that require separate and repeated logins due to system timeouts. These setups are onerous, but security itself is not the cause—the patchwork and outdated approach to it is. Privacy and security regulations should never hamper access to information necessary for patient care. Building in security at the start along with updating and improving systems should help this perception fade.

The goals of the meaningful use incentive programs, authorized by the HITECH Act, include promoting the use of EHRs, with the ability to share patient information on a national basis as the ultimate goal.

Many providers that have received funding from federal and state meaningful use programs have attested that they have completed security risk analyses and remediated as appropriate. However, it is unclear whether they included privacy and security provisions in their system planning and implementation efforts. Failure to include privacy and information security officers in these decisions and not requiring vendors to provide adequate security without affecting system timeliness and effectiveness has led many organizations to develop work-arounds after implementation or to ignore many security provisions. This adds to system cost and delays acceptance and implementation of new workflows and processes.

Healthcare technology vendors must be required to build in security from the beginning and be transparent when working with healthcare providers. Security solutions should be adopted as part of systems development and testing processes, as is common practice in software companies, engineering firms, and other businesses involved in building security into new products and services.

Trends and Changing Perceptions

Various trends and developments are affecting how healthcare privacy and information security are perceived and managed. Cybersecurity threats, cloud computing, mobile device technology, and the pervasiveness of social media directly affect healthcare operations and security programs. Another trend is the explosion of data, which makes safeguarding information assets increasingly

important. New and expanded entities, such as accountable care organizations and health information exchanges, have large appetites for data and data analytics. Researchers are collaborating and communicating across the globe, using more data and new types of data (e.g., genetic information). Data banks established and operated by commercial concerns store individual behavior and personal preference data. Government data collection efforts and activities, including data mining and data analytics, are increasing. Data collection via surveillance (e.g., cameras, global positioning systems, other monitoring devices) is on the rise. More types of data are being collected from more people in more ways, and being shared with more entities.

One result of these trends is the perception of privacy and information security as essential components of an organization's strategic planning efforts and risk assessment processes. Healthcare leaders must recognize these trends and develop methods for effectively assessing the impact of our changing world on organizations' security programs, strategic planning, and risk management processes.

The Effects and Consequences of Technology

Ethics and laws governing confidentiality evolved long before electronic medical records and health information exchanges were envisioned. The perception that protecting patient confidentiality is more difficult and burdensome because of advances in technology and the proliferation of networks exists. Healthcare organizations must strive to protect information to the fullest extent possible and to comply with all relevant state and federal laws.

Electronic health information systems allow increased access to health data and transmission of health data across various platforms and to many providers and others involved in patient care, treatment, and healthcare operations.

Clinicians in integrated delivery systems, accountable care organizations, and other networks have access to the confidential information of all patients within their systems. This information is transmitted via clinical repositories and shared databases to allow for safer and more efficient treatment. The challenge for clinicians is to use this technology for patient care while honoring and respecting patient confidentiality.

"Do not track" methodology, a mechanism that provides consumers the ability to adjust their computer settings to prevent advertisers and data brokers from tracking their online activities, has languished in Congress. Meanwhile, the amount of information about individuals has increased enormously. Even with laws that limit access to individuals' financial and medical information, such as the Fair Credit Reporting Act and HIPAA, data brokers can access and compile this information through other means.

Healthcare providers must be informed and aware of these various issues with respect to how they affect information privacy and security. Trustee and senior leadership involvement in program oversight and willingness to listen to privacy and information security professionals lead to greater understanding and awareness of how to make privacy and information security part of

an organization's culture of safety and quality. Leadership must establish expectations and hold workforce members and vendors accountable.

Questions About Privacy and Information Security

Use the following questions to promote discussion about your organization's privacy and information security principles and practices.

Does the mission statement address privacy and information security? If not, why? If yes, what purpose does the section that addresses privacy and information security serve? Do workforce members receive this information on a regular and ongoing basis?

Do organization leaders view HIPAA through a regulatory lens, with compliance and risk avoidance as the primary strategies, or as a basic patient and individual right that is consistent with the organization's mission and strategic goals? How do these differing perspectives affect daily operations?

Is the privacy and information security culture one of blaming or enabling?

How do privacy officers and ISOs communicate information about the programs to senior leaders, trustees, managers, clinicians, and workforce members? Which forms of communication do they use, and how frequently do they communicate? Is their tone negative (e.g., "Don't do this," "We can't do that because …") or positive (e.g., "You can protect patient information by applying these simple principles when using mobile devices")?

Do trustees and senior leaders receive regular, ongoing information about the progress of the privacy and information security programs beyond compliance statistics (e.g., number of inappropriate accesses to patient records, number of incidents and breaches, number of workforce members who have received HIPAA training)?

Describe organization strategies and plans for using mobile technology and ensuring secure communications when using mobile technology. How do privacy and security factor into strategies and plans?

When did trustees, senior leaders, and managers last review the organization's NPP?

Is the NPP included in orientation packets for new workforce members?

Is the NPP provided to BAs and subcontractors?

Is the NPP prominently posted in all organization locations and made available on the organization's website?

The Complete Guide to Healthcare Privacy and Information Security Governance

Phyllis A. Patrick, MBA, FACHE, CHC

Foreword by **Larry Ponemon, Ph.D.**

The Complete Guide to Healthcare Privacy and Information Security Governance provides essential information to help develop, implement, and evolve effective privacy and information security programs.

The interdisciplinary nature of healthcare processes and the consolidation of many functions across organizations makes this book useful for clinicians and healthcare managers, including privacy and information security officers, compliance officers, internal auditors, informatics officers, legal services staff, safety officers, quality officers, procurement officers, health information management professionals, information technology professionals, risk managers, researchers, educators, human resources management, and others responsible for safeguarding information assets.

This book also provides important information for senior leaders and trustees with respect to their role in and responsibility for overseeing privacy and information security programs.

> *What sets this book apart from others is its focus on the role of the board of directors and how critical its oversight responsibilities are to the management of these programs. [It] provides practical guidance on every aspect of healthcare governance. [W]hat makes this book such an indispensable and valuable resource is its recognition that the management of these programs requires many functions to collaborate to ensure successful outcomes. It should be read and frequently referenced by clinicians, healthcare managers, and informatics officers, as well as those in compliance, internal audit, legal services, and human resources management, and many others.*
>
> Larry Ponemon, PhD
> Chairman and Founder
> Ponemon Institute

CGHPISG

HCPro
a division of BLR
75 Sylvan Street | Suite A-101
Danvers, MA 01923
www.hcmarketplace.com

ISBN-13: 978-1-55645-160-7
90000
9 781556 451607