MARGRET AMATAYAKUL
MBA, RHIA, CHPS,CPHIT, CPEHR, CPHIE, FHIMSS

Guide to HIPAA Auditing Practical Tools for Privacy and Security Compliance

Guide to HIPAA Auditing: Practical Tools for Privacy and Security Compliance, Third Edition, is published by HCPro, a division of BLR

ISBN: 978-1-61569-283-5

Margret Amatayakul, MBA, RHIA, CHPS, CPEHR, FHIMSS, Author
Melissa Osborn, Product Director
Erin Callahan, Senior Director, Product
Elizabeth Petersen, Vice President
Matt Sharpe, Production Supervisor
Vincent Skyers, Design Manager
Vicki McMahan, Senior Graphic Designer
Michael McCalip, Layout/Graphic Design
Kelly Church, Cover Designer

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

Margret Amatayakul, MBA, RHIA, CHPS, CPEHR, FHIMSS

Margret Amatayakul is president of Margret\A Consulting, LLC, as well as cofounder and member of the board of examiners of Health IT Certification. She has extensive experience in contributing to privacy and security policy formulation as well as practical, on-the-ground work implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Having performed numerous assessments, including a recent increase in the number of reassessments and assessments sought by business associates, Amatayakul has had an opportunity to see some excellent best practices and some practices that might best be characterized as significant opportunities for improvement. She has also had the opportunity to participate as a contractor to the National Committee on Vital and Health Statistics, a statutory advisory body to the U.S. Department of Health and Human Services on HIPAA. Since 2000, she has witnessed firsthand the angst that many feel about protecting health information privacy as well as the challenges in guiding the diversity that makes up this nation and its healthcare delivery system.

Other aspects of Amatayakul's consulting practice include assisting in planning for, selecting, implementing, and optimizing use of electronic health records, personal health records, and health information exchange services and helping organizations adopt strategies for health reform as accountable care organizations.

Prior to establishing Margret\A Consulting in 1999, Amatayakul helped found and served as executive director of the Computer-based Patient Record Institute (CPRI), which grew out of

recommendations in the Institute of Medicine patient record study (1991). CPRI has now been folded into the Healthcare Information and Management Systems Society (HIMSS), continuing the Davies EHR Recognition Program that was initiated during her tenure. As associate executive director of the American Health Information Management Association (AHIMA), she was responsible for all aspects of academic preparation, continuing education, and certification, as well as the association's early advocacy efforts. She served the College of St. Scholastica as an adjunct professor, held a full-time tenured faculty position at the University of Illinois at Chicago, and was director of the medical record department at the Illinois Eye and Ear Infirmary.

Amatayakul observes that the revision to this popular book has come about for several reasons. First, any book relating to health information technology must be refreshed frequently. Second, much has changed with respect to privacy and security since the first and second editions, with new regulations, guidance, and stepped-up audits and enforcement of HIPAA. Finally, the incentive program for meaningful use of electronic health records has reinforced the importance of health information privacy and security through requirements for attesting to compliance with certain privacy rights, risk analysis, and technical security. As a result, many healthcare organizations want to shore up their practices and their documentation.

Introduction

Why Audit for HIPAA Privacy and Security Compliance?

The most important reason for an organization to conduct its own internal audit for compliance with any law is to ensure that the organization is, in fact, in compliance. However, many organizations take a chance and wait for an external audit or other—usually more egregious—event to occur before they consider conducting internal audits.

Healthcare organizations have not been immune to this posture. However, they are changing their perspective with respect to playing the waiting game as the stakes have become higher. There are ever more Health Insurance Portability and Accountability Act of 1996 (HIPAA) complaints being filed with the U.S. Department of Health and Human Services Office for Civil Rights (OCR). The number of large breaches (i.e., those affecting 500 or more individuals) increased by 138% between 2012 and 2013, and assessments and/or penalties have been significant, including one with both OCR and Federal Trade Commission (FTC) assessments and resolutions. The federal incentive program for making meaningful use of electronic health record (EHR) technology (collectively being referred to as meaningful use) requires performance of a security risk analysis. Incentive monies have been returned on the basis of incentive program audits with either the lack of or an incomplete security risk analysis almost always a factor.

In addition to the threat of enforcement looming closer to home, many healthcare organizations are recognizing the business case for compliance assurance. Patients have always been concerned about the privacy and security of their health information, but credit card theft, identity theft in general,

and medical identity theft in particular are increasing. New laws (i.e., regulations) continue to focus on strengthening privacy and security practices and extending these more directly to business associates. As such, healthcare organizations increasingly are seeking to conduct audits and to be more proactive with respect to risk mitigation.

Where Does It Say We Must Audit for Compliance?

The HIPAA Privacy and Security Rules do not explicitly describe a compliance assurance program or ongoing auditing and monitoring. However, several specific standards require covered entities to ensure the following:

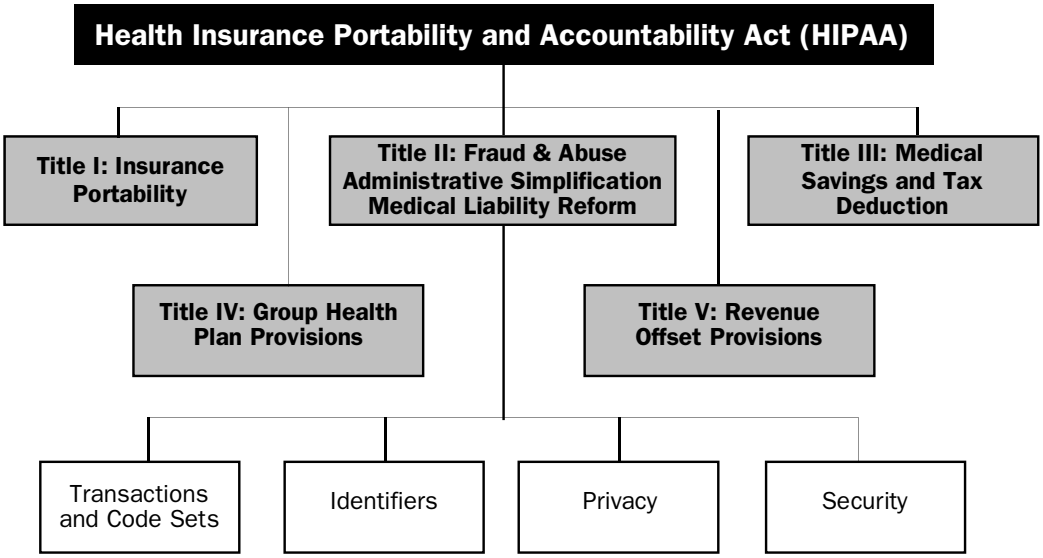
"[U]ses and disclosures are consistent with the notice of privacy practices" [45 *CFR* 164.502(i)]

"[S]ecurity measures … be reviewed and modified as needed to continue provision of reasonable and appropriate protection" [45 *CFR* 164.306(e)]

"[A] periodic technical and nontechnical evaluation [be performed] … in response to environmental or operational changes affecting the security of the electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements" [45 *CFR* 164.308(a)(8)]

HIPAA is also broader than the administrative simplification provisions. Refer to Figure I.1 for a chart that illustrates this. HIPAA's fraud and abuse provisions prompted healthcare-covered entities to create a corporate compliance structure. These provisions authorize the U.S. Department of Health and Human Services' Office of Inspector General to conduct investigations, audits, and evaluations related to healthcare fraud. These provisions recommend a comprehensive compliance program. As a result, many healthcare organizations created corporate compliance offices and designated corporate compliance officers. The HIPAA administrative simplification provisions for privacy and security differ from its fraud and abuse provisions, but there is no difference in the need for ongoing compliance.

Figure I.1 | Health Insurance Portability and Accountability Act of 1996 (HIPAA)



Source: Margret\A Consulting, LLC. Reprinted with permission.

In addition to HIPAA, 47 states have enacted data breach notification laws, requiring companies that maintain any form of personal information about their customers, clients, or patients to notify them of any incident involving disclosure of such information. The primary intent is reducing identity theft, or at least mitigating the harm that may arise from such theft. California, the first state to enact a data breach law, also enacted patient privacy laws that set a precedent for other states. California explicitly describes healthcare facilities' obligation to notify patients of data breaches and to take reasonable steps to monitor and stop inappropriate access. It requires reporting breaches when data are acquired or simply accessed (i.e., viewed only). As many states build state-based health information exchange (HIE) organizations (HIO), they are also enacting new laws aimed at reducing privacy and security risk. These new laws require encryption of sensitive personal information that is transmitted electronically or stored on portable devices. HITECH's federal data breach notification requirement for unsecured health information does not explicitly require that health information be encrypted, but its definition of securing health information during transmission is essentially encryption. The federal breach notification requirement has also undergone some modifications to add clarity via the Omnibus Rule.

The FTC is also stepping up requirements for financial institutions and other organizations that offer consumer credit to develop and implement written identity theft prevention programs. The agency's "Red Flag and Address Discrepancy Rules" define, with great specificity, the obligations of creditors. Although not all healthcare organizations meet the definition of creditor, many have adopted the principles of the Red Flags Rules because the risk of both medical and financial harm to patients and financial harm to an organization attributable to medical identity theft can be immense.

Compliance is ongoing observation of regulatory requirements. An organization is subject to enforcement penalties when found to be not in compliance. In some cases, penalties may not derive

directly from the compliance requirements, but from the cost of recovering from a breach. Further, the effect on an organization's reputation can be significant.

As observed in the HIPAA Security Rule's evaluation standard, regular environmental and operational changes affect the nature of risk that healthcare organizations face. Compliance is continuously challenged through changes in workforce turnover, new information systems, and new and different external pressures. Compliance should not be left to mere chance.

How Can This Book Help?

Executive management support is critical regardless of laws or philosophy of good data stewardship with which your organization is expected to comply and regardless of how you structure your privacy and security compliance assurance program. A workable plan, adequate resources, and tools to help you determine your current compliance status, identify potential issues, make compliance improvements, and document your efforts will put you in good stead for any formal audit that federal regulators may conduct or for any legal action that requires you to substantiate your efforts.

This book will help you do the following:

- Build the business case for compliance assurance
- Understand and communicate to all concerned, including those within your organization and your business associates, the purpose and nature of auditing and monitoring for compliance with privacy and security measures
- Construct an appropriately resourced privacy and security compliance assurance program
- Use tools to effectively plan for, conduct, and document the process for auditing and monitoring privacy and security compliance
- Close the feedback loop when potential issues arise and necessitate privacy and security compliance assurance improvements
- Identify and evaluate external resources for use in constructing your privacy and security compliance assurance program

Access additional resources in the online Appendix at *www.hcpro.com/downloads/11642*.

Building the Business Case for Compliance Assurance

Generally, one considers developing a business case when initiating a project (i.e., something with a defined beginning and end) or task (i.e., something expected to be an ongoing performance requirement). For healthcare organizations, compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules has been an expected ongoing performance requirement since 2003 and 2005, respectively. Despite stepped-up enforcement of HIPAA, audits initiated for the meaningful use program, and the rising cost of managing privacy and security complaints, breaches, and new regulatory requirements, many information privacy and security officials find that appropriately resourcing this ongoing task is a constant battle. Even without HIPAA Omnibus Rule requirements, the meaningful use program requirement for a security risk analysis, and increasing requirements for enhanced privacy and security in health information exchanges, the world in and around healthcare is increasingly adopting new forms of information technology (IT), and with them the potential for greater risk. The Identity Theft Resource Center reports that 43% of the identity thefts reported in the United States in 2013 were medical-related, usually as a result of hacking into computer networks or stealing laptop computers. Medical identity theft is not only the fastest-growing crime in the United States, but has both medical and financial ramifications for patients and financial ramifications for providers.

As a result of the increasing risks in the landscape of healthcare, information privacy and security officials must maintain an ongoing business case that continuously justifies compliance assurance resources. Scanning the internal and external environment for changes that affect the privacy and security of protected health information (PHI) is a routine part of information privacy and security

officials' jobs. But with the pace of change in technology getting faster, such as rapid adoption of cloud computing, increasing demand to "bring your own devices," social media usage, and big data analytics aggregating data from providers with results tightly associated with financial risk, extra vigilance is required. Making the results of these environmental scans widely known throughout an organization can promote continual awareness and drive compliance in many ways.

This chapter does the following:

- Defines the purpose of a compliance assurance program
- Describes the need for a compliance assurance program for privacy and security
- Discusses the importance of building a business case for resourcing the privacy and security compliance assurance program
- Provides tools to construct a business case that justifies periodic changes and enhancements in the privacy and security compliance assurance program
- Offers suggestions for conveying the message in the business case to garner support throughout the organization for attention to privacy and security measures

Purpose of a Compliance Assurance Program

A compliance assurance program guides an organization in performing its responsibilities relative to legal, regulatory, and ethical requirements. In 2012, the U.S. Department of Health and Human Services' (HHS) Office of Inspector General (OIG) created a "Compliance 101" website to reiterate much of what it published in 1998 in its *Compliance Program Guidance for Hospitals,* and subsequently, in 2005 in its *Supplemental Compliance Program Guidance for Hospitals.* While largely focused on fraud and abuse, the website and both guidance documents describe several important benefits of a compliance assurance program. For example, a compliance assurance program does the following:

- Guides the ethical leadership of an organization
- Assists in identifying weaknesses in systems and management to enable establishment of internal controls
- Helps an organization concretely demonstrate commitment to responsible corporate conduct
- Provides an accurate view of behavior relative to specific requirements
- Creates a centralized source for distributing information about compliance
- Develops methodology that encourages employees to report potential problems
- Develops procedures that allow the prompt, thorough investigation of alleged misconduct
- Initiates immediate and appropriate corrective action
- Minimizes loss through early detection and reporting and reduces exposure to civil damages and penalties, criminal sanctions, and administrative remedies

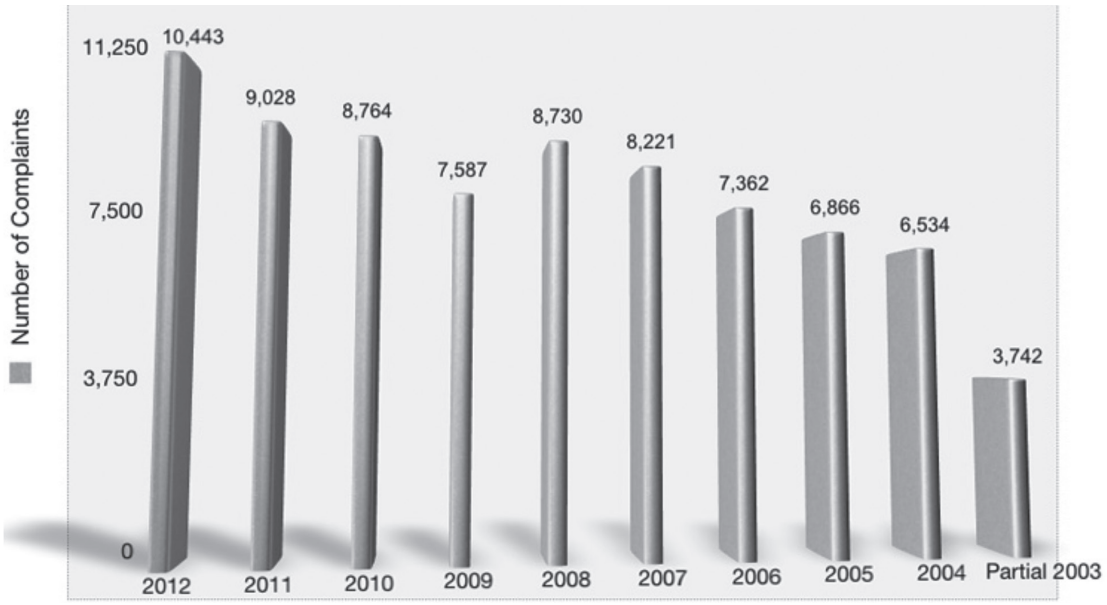
Need for a Privacy and Security Compliance Assurance Program

The HIPAA Privacy and Security Rules, subsequent enforcement regulations, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Omnibus Rule set forth requirements for compliance with privacy and security standards to protect individually identifiable health information held by covered entities, business associates, and, at least to some extent, others, such as personal health record vendors. A fundamental premise for a compliance assurance program targeted at privacy and security is as follows:

- Covered entities and potentially business associates acting as agents for covered entities may receive complaints from their patients/customers or any other member of the public concerning their privacy and security practices. No fines or penalties are directly associated with a complaint filed exclusively with an organization, but there is a cost associated with responding to each complaint, tracking complaints over time, and mitigating the risks associated with complaints. The risk that the complaint will be escalated to the HHS Office for Civil Rights (OCR) is always present, at a minimum requiring an organization to develop a response to a letter from OCR and to potentially manage a corrective action plan.
- OCR can impose settlement fees, fines, and/or criminal penalties for noncompliance with privacy and security rules, including breaches.
- The Federal Trade Commission (FTC) can impose settlement fees or fines for breaches associated with commercial personal health records and can use its general enforcement authority surrounding consumer protection and deceptive trade practices to very broadly address issues where consumer trust has been violated.
- The Centers for Medicare & Medicaid Services (CMS) can impose fines for noncompliance with the other HIPAA administrative simplification rules (i.e., transactions and code sets and identifiers). CMS also requires return of incentive monies under the meaningful use program if it finds that eligible hospitals or professionals have falsely attested to compliance with program requirements. This is an all-or-nothing situation; even if a provider's only missing element is a security risk analysis, all incentive money must be returned.

States' attorneys general also can enforce HIPAA. Only one state's attorney general has taken such enforcement action to date, but the potential for more to do so exists. The OCR website illustrates that privacy complaints have continued to rise between April 2003 and December 2012. Refer to Figure 1.1. Visit *www.hhs.gov/ocr/privacy/hipaa/enforcement* for additional information about enforcement.

Figure 1.1 | Complaints Received by Calendar Year



Source: U.S. Department of Heatlth and Human Services. *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html*

A vast majority of the complaints are resolved either because no Privacy Rule violation occurred or evidence supplied by the covered entity indicates compliance with the rule. The remaining complaints, the nature of which is described in Figure 1.2, result in the covered entity supplying the OCR with a corrective action plan and potential settlement fees or fines.

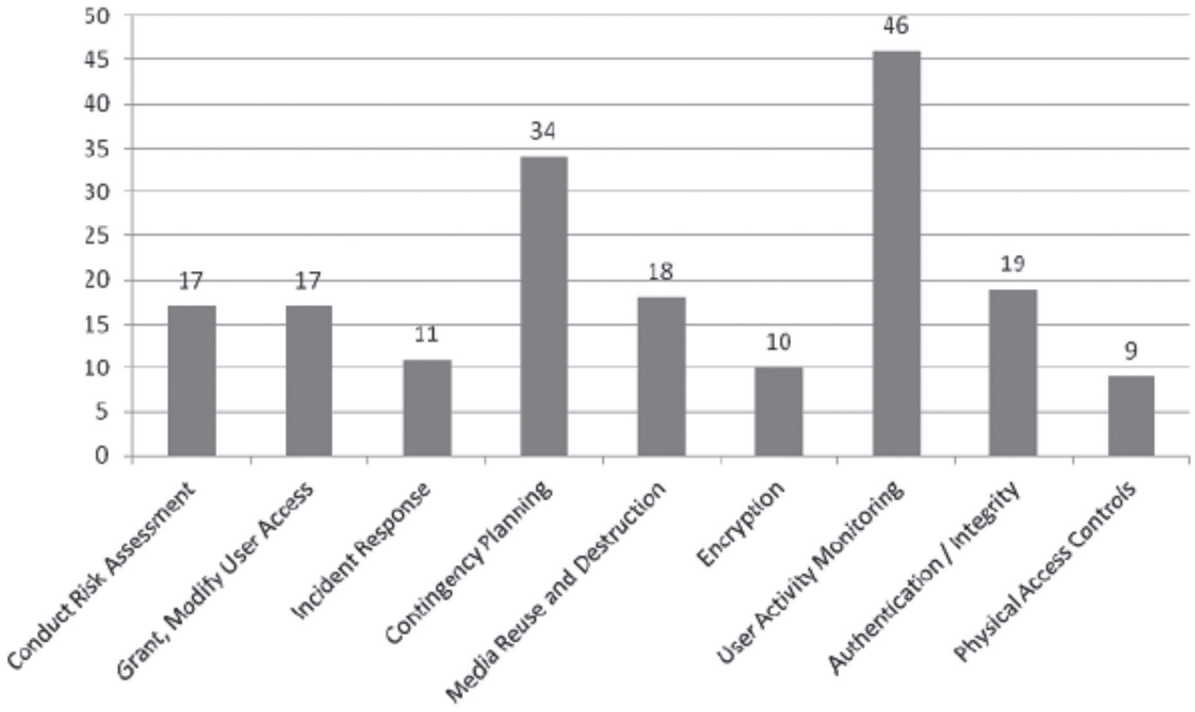
Figure 1.2 | Top Five Issues in Investigated Cases Closed With Corrective Action, by Calendar Year

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2010	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2009	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity
2008	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity
2007	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2006	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2005	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Mitigation
2004	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Authorizations
partial year 2003	Safeguards	Impermissible Uses & Disclosures	Access	Notice	Minimum Necessary

Source: U.S. Department of Health and Human Services.
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/top5issues.html

OCR took over responsibility for enforcing the HIPAA Security Rule from CMS during July 2009. CMS received 379 Security Rule complaints (accounting for more than 525 violations) between 2005 and 2007. Today, OCR indicates that many privacy complaint investigations also reveal security issues. Other than the security findings from the 2012 pilot audits conducted by OCR, it does not report on Security Rule complaints. Refer to Figure 1.3.

Figure 1.3 | 2012 OCR Security Audit Findings



Source: U.S. Department of Health and Human Services.
http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2--2_lsanches_ocr--audit.pdf

This should not be construed that OCR does not consider security important. Rather, the public primarily understands security from the perspective of confidentiality, is not necessarily aware that a separate Security Rule exists, and hence is more inclined to file a privacy complaint than a security complaint. Although OCR has never stated this, it may also be applying a bit of psychology here—where reporting the small number of direct security complaints may signal to the industry that security is not as important as privacy.

OCR also maintains a website that tracks large breaches. In early 2014, its website (*www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html*) revealed that more than 800 breaches potentially compromising 67.7 million individuals' health records had occurred since tracking began in 2009. Refer to Figure 1.4 for a summary of breach types and locations.

Figure 1.4 | Types and Locations of Large Breaches

Type of Breach	Location of Breach
Hacking/IT incidents	Backup tapes
Improper disposal	CDs
Theft/loss	Desktop computers
Unauthorized access/disclosure	Email
Unknown	Films
	Laptop computers
	Network servers
	Paper
	Other portable devices
	Other

Source: U.S. Department of Health and Human Services. Abstracted from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

As of early 2014, HHS entered into 17 settlements (including one for a small breach) and has levied one civil money penalty (CMP). The number of settlements has increased annually. The total value of settlements exceeds $10 million and the one CMP levied was in the amount of $4.3 million. The sole settlement involving a state attorney general action was in the amount of $2.5 million and included FTC requirements for biennial security risk assessment reporting to the FTC for 20 years.

Note that a settlement amount is only a fraction of the cost of breach management to a covered entity or business associate. Few breaches have resulted in a settlement or CMP. However, direct costs for managing any reportable breach include notification and risk mitigation. This usually includes notification letter creation and mailing and paying for discounted or free credit monitoring and/or financial counseling services offered to those harmed. It also may include fees paid to attorneys to advise the organization how to address liabilities, consultants to conduct a forensic analysis of the cause of the breach, public relations firms to help respond to media and public inquiries, and temporary call centers to handle increased call volume. In addition, there can be reputational harm that could result in loss of customers. The Ponemon Institute estimates that cost of a breach per record is $188. The average number of records breached during a privacy and/or security incident in 2012 was 23,647. The total cost of managing one breach of this size would be more than $4.4 million. MeriTalk's Health IT Community used data from a Health Information Management Systems Society (HIMSS) survey conducted in 2013 to estimate that the average cost of a healthcare breach is $810,000. Either amount is something no healthcare organization wants to incur if it can be avoided.

A compliance assurance program for privacy and security enables an organization to respond to complaints. More importantly, it supports the organization's ability to comply with the HIPAA

Privacy and Security Rules by identifying potential areas of increased risk by assessing the nature of the privacy and security complaints and breaches reported to OCR, identifying its own internal threats and vulnerabilities, and tailoring a compliance program that improves the privacy and security it affords the PHI it retains and may transmit. Without such a program, managing appropriate controls is difficult and it is virtually impossible to provide documentary evidence of compliance in the event of a complaint.

Building a Business Case for Resourcing a Compliance Assurance Program

A business case for resourcing a compliance assurance program for privacy and security should be possible solely on the basis of the need to respond to complaints made directly to a covered entity (or business associate acting as an agent of a covered entity). However, despite stepped-up enforcement and periodic audits required by HITECH, industry experts still anticipate that a more proactive process for compliance may not be taken until an untoward event occurs. Consequently, other avenues for substantiating the importance of privacy and security measures are necessary and readily available, several of which have already been noted.

Information privacy and security officials may find it necessary to go beyond information about HIPAA Privacy and Security Rule enforcement in making the business case. Monitoring the general security industry and relating those risks to healthcare privacy and security are important when doing so. Consider the following:

- Track information about identity theft and medical identity theft. A blog entitled AllClearID Alert Network tracks medical identity theft and also provides tips on protections. For example, the March 27, 2014, post, "3 Things You May Not Want to Share With Your Doctor" (*https://www.allclearid.com/blog/tag/medical-identity-theft-2*) states that there were 1.85 million victims of medical identity theft in 2012 (up from 1.49 million in 2011), with consequences including 50% of victims reporting paying out-of-pocket to their health plan or insurer to restore coverage, 20% reporting a drop in credit score, 20% reporting lost productivity due to time spent to resolve the issue, 15% reporting legal fees needed to help resolve issues, and 8% seeing their health premiums increase. From the clinical perspective, 18% of victims experienced mistreatment of an illness due to inaccuracies in their medical records. The source of medical identity theft can be a HIPAA covered entity or business associate and other sources. Patients may not know the source of the theft and could potentially blame a covered entity, so it behooves covered entities to educate their patients. For example, the blog cited notes that medical identity theft stemming from attacks on computer games and consoles when clicking on a link to play a game resulted in malware downloads that supplied attackers with personal information.

- Review routinely issued reports about privacy and security from reliable sources, such as the following:
  - The Electronic Privacy Information Center (EPIC) tracks emerging privacy and civil liberties issues at *http://epic.org/*.
  - The Center for Democracy and Technology (CTG) manages the Center for Democracy & Technology Health Privacy Project and tracks privacy issues in healthcare at *www.cdt.org/issue/health-privacy.*
  - HIMSS publishes the results of its annual survey on security. The 2103 report is available at *http://himss.files.cms-plus.com/2013_HIMSS_Security_Survey.pdf*.
  - The Ponemon Institute tracks a variety of industries, including specifically healthcare. Its 2014 report is available at *http://lpa.idexpertscorp.com/acton/attachment/6200/f-012c/1/-/-/-/-/ID%20Experts%204th%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%20%281%29.pdf*.
  - The Ponemon Institute also collaborates with Symantec to develop its findings on costs of breaches. Visit *www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf*.
  - Verizon also publishes reports on breaches, such as one on sources of breaches and technical controls. Visit *www.verizonenterprise.com/DBIR/2013/*.

Accurate representation of findings and judicious use of this information are important when using these and other resources. For example, the 2013 HIMSS survey reports "snooping staff still a big concern." An earlier HIMSS survey found that 35% of the top breaches reported by survey respondents were due to employees snooping in fellow employees' medical records and 27% of breaches were due to employees snooping in friends' and relatives' records. These surveys also found that 79% of respondents were "somewhat concerned" or "very concerned" that their existing controls do not enable timely detection of breach of PHI. This can be useful information to support a compliance assurance program in general and strengthen access controls/audit logging and training in particular.

However, the surveys also found that nearly half of the respondents still spend 3% or less of their overall IT budget on security initiatives, although the other half indicate an increase in their budgets. Budget numbers could be construed as justification to not spend more than others in the industry. If an organization's budget is already low, the average budget might be useful with respect to increasing the budget. However, if the budget is already higher than the average, an increase would require justification with proven results that are often more difficult to identify.

Constructing the Business Case

The purpose of a business case is providing justification for expending resources. The business case can take many forms, including, but not limited to the following:

- A comprehensive study of the analysis of an organization's strengths, weaknesses, opportunities, and threats with respect to the proposed project or program
- A formal cost-benefit analysis with financial evidence of return on investment for the program
- Documentation of alternative courses of action considered, including the risk of doing nothing
- A formal request for a decision with respect to the actions proposed

Alternatively, a business case can be a brief, verbal argument that explains why a project or program is necessary.

Something between a comprehensive study and a brief, verbal argument is probably what is necessary to persuade management to expend more time, focus, commitment, and actual resources on privacy and security in most healthcare organizations. Ideally, a major incident is not the impetus. Refer to Figure 1.5 for information that is helpful with respect to building a business case for a privacy and security compliance assurance program.

Information privacy and security officers who want to do more than simply respond to complaints or incidents and institute proactive compliance assurance programs should compile evidence supporting the need for a formal privacy and security program. This evidence can come from general concerns about privacy, identity theft, and data breaches. However, a more compelling business case is possible if this type of information is used to compile a checklist of risks for determining the likelihood of their occurrence and potential for harm in an organization. The ability to relate risks to reality improves the ability to justify the need for and obtain heightened protections.

Making the business case real for an organization may require investing time in conducting an assessment of the current state of affairs. A comprehensive assessment may not be necessary. Instead, a focused study of one or two areas where an organization is thought to be at most risk may suffice. For example, an organization that has adopted an electronic health record (EHR) system but has not adopted role-based access controls should conduct a proactive audit log analysis. A first finding may be that audit logging does not occur or that audit logging identifies only persons who logged onto the network. Where audit logs exist, formulate a plan to review audit logs from randomly selected dates, times, and locations to determine the extent of inappropriate access. Such

Figure 1.5 | Business Case for Privacy and Security Compliance Assurance Program

Executive summary: Briefly describe the purpose for the (enhanced) privacy and security compliance assurance program for your organization, and how that differs from today. For example, if an IPO spends 90% of its time responding to complaints and 10% time training new employees, the proposed program may reduce volume of complaints by half through a joint IPO and ISO proactive monitoring program, where each devotes 30%of its time to monitoring; 45% responding to complaints; and 25% training new employees and providing reminders to existing staff. State specifically what action you want executive leadership to take upon review of this business case. For example, approval for biannual external assessment, .25 FTE staff for one year to assist in responding to complaints while program is initiated, and specified software tools. Request support for consistently applied sanction policies and two 10-minute presentations per year by the CEO on the importance of information privacy and security management.
Rationale: Describe the current environment and how that has or can be expected to affect organization. Make clear assumptions, facts, estimates, and projections. For example, you may identify that impermissible uses and disclosures is the most common complaint directed to OCR, and that a review of audit trails reveals 3% of employees may make an unauthorized access.
Costs: Identify specific incremental costs for enhanced or new program. Include additional staff, consultants, software, hardware, subscriptions, training programs, certifications, etc. Project expenditures for three to five years depending on your organization's typical planning horizon.
Benefits: Identify specific benefits, such as cost reductions, discounts available, contributions to profit, etc. If benefits have specific dependencies, identify those explicitly. For example, if a benefit only accrues if an incident occurs but it costs less to mitigate because of the proposed program.
Critical success factors: Define specific, measurable, attainable, realistic, and timely (S.M.A.R.T.) goals. For example, this program will reduce complaints concerning disclosures to individuals involved in care of a patient by 75% within three months of instituting and monitoring use of a "family code" process.
Dependencies: Describe internal (e.g., staff training, commitment to requiring use of a security token for remote access) and external (e.g., tighter state regulation) factors that affect success of the program.
Options: Describe other structures, resources, tools, etc., that may potentially achieve the desired benefits and why all but the one proposed was rejected.
Deliverables: Describe regular reporting and other visible means that will describe how the program is working and achieving the intended benefits.

Source: Margret\A Consulting, LLC. Reprinted with permission.

monitoring is time-consuming and potentially prone to error without automated pattern analysis tools, so reviewing a sufficient number of audit logs with a preplanned set of criteria to obtain accurate results is essential. If your organization does not conduct proactive audit log monitoring, as many do not, consider requesting approval for conducting the monitoring program you have formulated. The results illustrate the direct relationship between adopting role-based access controls and reducing what OCR reports as the most frequent complaints, specifically those pertaining to the following:

- Impermissible uses and disclosures
- Safeguards
- Minimum necessary
- Information access management
- Access controls

In addition to demonstrating which risks exist in an environment, thinking about how a compliance assurance program can best be structured is necessary to accomplish the stated goal of protection and to optimize resources.

Most hospitals already have corporate compliance programs, information privacy officers, and information security officers. Must these be three separate functions? Or could they be two functions, or only one? Some information privacy and security officers fear that merging with other compliance elements within an organization will result in further deterioration of their focus. This may not be the case. Larger compliance programs may have sufficient clout to enhance the privacy and security focus. Alternatively, rethinking organizational relationships may be necessary if a larger compliance program is not working well. Either way, a business case should not create the perception that any one individual is attempting to build an empire, but instead should ensure that issues are addressed. The key is thinking creatively, rather than traditionally.

Describing time commitments and costs to an organization is also an essential element of a business plan. Using readily available generic information provides guidance, but demonstrating an efficient approach that will work best in a particular environment and minimizes additional direct expenditures is essential.

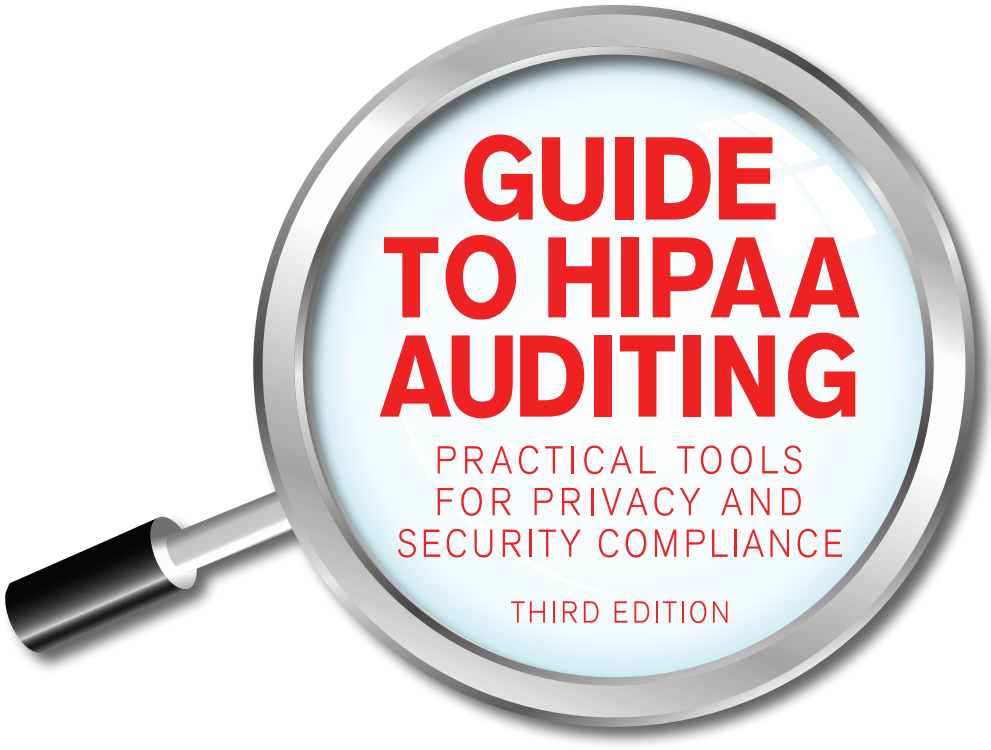
Conveying the Message

A final element in any business case construction is ensuring inclusion of materials that can be used for a variety of venues and purposes. Numbers and a rationale to support creation or enhancement of a compliance assurance program for privacy and security will be necessary at capital budgeting time.

Ensure your ability to continually justify or enhance your position for recommending or sustaining such a program throughout the year. Toot your own horn when the compliance program has successfully thwarted a potential incident. Be prepared with unique facts about your organization's privacy and security position when privacy or security incidents elsewhere make headlines. This is both demonstrable evidence of the importance of a compliance assurance program and a teachable moment.

Conclusion

A compliance assurance program for privacy and security provides proactive readiness for any eventuality. The Joint Commission now conducts unannounced surveys, and HITECH requires periodic privacy and security audits. Audits for other compliance issues can also spill over into privacy and security areas, such as meaningful use. Many providers are aware that any audit for any purpose can lead to discovery of other compliance issues. Multiple federal agencies can become involved. Even if each one does not impose direct financial penalties, other penalties that are equally or more expensive and certainly time-consuming are possible. Regular internal audits and corrective actions are much easier and less costly than federally imposed corrective action plans, breach resolutions, and audits, or even breach notifications that do not result in federal action.



MARGRET AMATAYAKUL
MBA, RHIA, CHPS, CPHIT, CPEHR, CPHIE, FHIMSS

Workforce turnover, new information systems, and external forces are continuous compliance challenges. And with HIPAA audits increasing and Office for Civil Rights (OCR) monetary settlements steadily increasing, the risk of appearing on OCR's "wall of shame" is greater than ever. OCR continues to investigate complaints and assess penalties–with fines topping $4.8 million for alleged violations during a joint arrangement involving two covered entities. The first step to ensuring HIPAA compliance is developing an effective risk analysis and management process that identifies threats, corrects vulnerabilities, and protects your patients.

Guide to HIPAA Auditing: Practical Tools for Privacy and Security Compliance, Third Edition, will help you build a successful HIPAA compliance auditing and monitoring program, identify potential risks, improve your compliance program, and document activities at your organization–putting you in good standing for any government audit or litigation that requires you to substantiate your efforts.

This essential resource:

- Delivers a comprehensive combination of up-to-date information and tools that facilitate HIPAA and meaningful use attestation audit preparation
- Provides up-to-date information to help you prepare for the American Health Information Management Association's CHPS® (Certified in Healthcare Privacy and Security) certification examination
- Explains how to conduct effective internal audits that help ensure your facility is ready for a government audit
- Includes updated tools and sample plans to identify and address potential risks

GHA3

ISBN-13: 978-1-61569-283-5

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