Mitigating Risk for Privacy and Security Compliance

Kelly McLendon, RHIA, CHPS
Founder, Health Information Xperts

Lucy Mancini Newell, MBA, FHIMSS
Managing Partner

October, 2011
Mitigating Risk for Privacy and Security Compliance

Introduction

For many decades, healthcare providers and organizations (i.e. hospitals and health systems) have been obligated to safeguard both the privacy and security of patient information. While efforts in a paper-based record were onerous enough, the fast paced digitization and exchange of patient information through Electronic Health Records has only served to increase the challenge to maintain privacy and security for that patient information. The amount of electronic protected health information (ePHI) has grown exponentially and so have the requirements for compliance.

There is a tight linkage between and among all the connecting points required to achieve privacy and security compliance:

1. policies,
2. procedures,
3. operational processes across healthcare environments,
4. technology, and
5. information systems and technology.

All healthcare providers and business associates should undertake discussions with their Chief Compliance Officer, Chief Information Officer, Risk Manager, etc. to identify the current state of these linkages within their organization and to determine whether some of these may also present areas of potential risk. Ultimately, the planning efforts related to compliance must include input and information from all the related disciplines that manage and maintain the proper organizational levels of compliance.

For the purposes of this white paper, it is, however, timely to focus the conversation about privacy and security on how best to mitigate potential risks that might arise in your organization. Compliance efforts continue to become more complex and require on-going investment of resources to address these requirements. We have identified seven potential impacts which can result from challenges related to HIPAA privacy and security.

We encourage each organization to review both privacy and security requirements with a comprehensive approach to ensure on-going compliance of HIPAA privacy and security while leveraging our suggested areas of potential risk.
Mitigating Risk Associated with Privacy and Security

How did we get here?

To accompany the growing levels of electronic protected health information (ePHI), legislation, both at the federal and state level, has been passed to provide patients with a measure of comfort that their privacy will be maintained as their records are increasingly computer-based. The original intent of the legislation was to ensure a focus on privacy and security during the implementation of Electronic Health Records (EHRs) and, thus, tying these mandates to the present day, incentive compensation of healthcare organizations that have attained meaningful use of certified EHRs.

To ensure privacy and security compliance, both state Attorney Generals and their staff as well as a force of Federal enforcement agents are assigned to audit and investigate potential violations. In addition, there is a statutory requirement within the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 that mandates the reporting of notification of breaches of unsecured protected health information. Most recently, a report has been issued by the U.S. Department of Health and Human Services, Office for Civil Rights and presented to various committees in Congress to comply with the required oversight identified in the legislation.

[Note: Name of Report: Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2009 and 2010]

In September, 2011, we have additional evidence of the federal commitment to preserving the trust of patient-consumers in their most recent document, the 2011-2015 Office of the National Coordinator for Healthcare Information Technology Strategic Plan. This document clearly paints an overview of why the U.S. government believes ePHI must be protected. The report further identifies the planned steps for further expansion of the regulatory environment as well as pursuit of better technology solutions to help manage compliance with these statues and rules.
Mitigating Risk Associated with Privacy and Security

In preparation for your organization’s review and assessment of privacy and security protocols, processes and technologies, we have identified seven areas where potential risks might arise. While there may be additional potential risks, each organization can use this information to augment their internal method of annually reviewing all areas supporting Privacy and Security requirements.

1. Organizational Liability
2. Financial Impact / Cost
3. Processes to Detect, Inform and Escalate
4. Operational Efficiency
5. Technical Integrity
6. Employee and Physician Education
7. Public Relations / Consumer Confidence

1. Organizational Liability

As with many other compliance initiatives, there will be organizational penalties applied for potential privacy violations and breaches. We do know that both federal and state government efforts have been accelerating. The possible penalties may include not only a monetary fine but, perhaps the greater penalty of negative reaction from the community at large. The impact that this liability can cause the reputation of a hospital or health system be harmed and the repercussions can be many.

These two types of organizational liabilities can create a cascade of events and reactions that will require substantial resources to help reverse and minimize the impact. In addition, there may be some long term impacts should the local community believe there is a crisis of confidence. As a result of learning about any wrongful disclosure, breach or other privacy or security issues which are made public, both executives and governing board will need to mobilize and introduce both short-term and long term measures to address the concern.

One of the more public liabilities associated with privacy and security is the HIPAA rules that mandate the publication of certain breaches on not only the federal OCR website, but also local media so the stakes for healthcare organizations with large privacy breaches is an intimidating outcome.

Clearly all HIPAA requests and complaints are important. Proactive, well documented investigation and continuous monitoring of any events which are identified at your organization will require oversight and regular reporting to your Privacy or Security Officers for compliance.
Mitigating Risk Associated with Privacy and Security

2. Financial Impact / Cost

Financial impact can be viewed like the two sides of a coin: either cost avoidance or investment tied to the prevention of negative effects resulting from risk. There is no approach that will have insignificant expense when it applies to maintaining all the requirements of HIPAA privacy and security. Some of the investment will be required for:

- infrastructure,
- processes,
- policies,
- on-going education for the organization,
- staff skills, and
- experience.

It is important to ensure that specific types of resources are actively engaged to either prevent or assist in reversing the effects of a privacy violation: Legal Counsel, Communications and Marketing resources, external Compliance expertise specific to privacy and security, etc..

Fines potentially can add up to millions of dollars for each violation. In addition, states can routinely impose fines for simple wrongful disclosures such as mis-directed faxes. The fine for this type of wrongful disclosure can be at least $25,000 per event. Plus the cost of breach notification can exceed $1 per patient breached. In the case of large breaches this can add up to a staggering expense from fines and notification costs, just for a single incident.

Supporting and maintaining a compliance effort requires both long-term resources and effort to safeguard any potential, negative financial impact. Fines are an obvious type of negative impact yet there are others. There can also be other cumulative financial impacts that may result if patients are no longer referred by physicians once they are made aware of such an event and the community at large may lose confidence in the institution resulting in further reductions in referrals, patients or their visits.

3. Processes to Detect, Inform and Escalate

A proactive monitoring program should be in place to serve as the framework by which HIPAA privacy and security can have the required oversight as well as tasks/activities that support vigilance through best practices and policies. In addition, the processes that are in place may be manual or may be supported by a technology solution to facilitate logging and tracking of investigations. While manual detection and management of events will be labor intensive, it is possible that such an approach be viable.
Mitigating Risk Associated with Privacy and Security

It may be preferable as requirements become more complex that an automated solution be sought to ensure that the appropriate documentation is managed and all subsequent follow-up and reporting is contained in an organized fashion and facilitates any required oversight by designated professionals and executives.

Automation of the management and documenting privacy events that have been discovered is a new area for technology, prior to the ramp up in electronic records, tightening of rules and enforcement there was little demand for technology as the penalties were non-existent. That has all changed since the introduction of HITECH and the HIPAA expansion. Now automation of privacy audit log monitoring, security information and event monitoring are being combined with detailed investigation and reporting documentation in sophisticated computer applications.

Knowing when to escalate discovered events into incidents which may require involvement from the highest levels of the organization is much more easily accomplished when accurate and complete documentation and reporting mechanisms are utilized. Under the new HIPAA expanded rules, especially in the case of wrongful disclosure and breaches timing is crucial to stay within compliance and avoid fines and negative publicity, therefore it follows that becoming increasingly formalized and automated is necessary to prevent the downsides that can occur if mandated time frames are missed.

4. Operational Efficiency

Although manual documentation and processes can always be in place and provide the type of framework by which privacy and security can be managed, operational efficiency can be increased with privacy automation. Depending upon an organization’s resource allocation and the elevating number of tasks privacy and security professionals are faced with, an automated solution to tracking and managing privacy and security events is an important investment to the organization’s portfolio of tools and applications.

The time for multiple, disparate, cobbled-together spreadsheets or very simple database programs that are used to manage privacy and security events are coming to an end. It is becoming inefficient and labor intensive to not only investigate, but also document and subsequently report upon discovered privacy and security events. Healthcare organizations have recently reported that the OCR enforcement process has demanded huge volumes of reported data, which if manually processed can be very inefficient and costly to produce.
Mitigating Risk Associated with Privacy and Security

5. Technical Integrity

Working with the Chief Information Officer, an executive can confirm the various approaches in place to safeguard access to patient information throughout the organization. Software applications should have audit trails which document access to and entry of patient information. The technical infrastructure will have various additional safeguards and layers of security to further protection of the patient information.

As part of a routine review of all organizational privacy and security efforts, all technical updates should be corroborated and documented. (Note: Mobile devices have introduced an additional level of complexity for healthcare professionals since malicious hacking of these devices has escalated over time).

6. Employee and Physician Education

Healthcare professionals are typically provided routine, comprehensive, regularly scheduled continuing education on a variety of topics related to working and interacting in a healthcare environment. Specific privacy and security compliance education should be included including specifics of wrongful disclosure and breach policies and procedures.

Workforce education can be made available through a variety of venues such as hospital / health system intranet, internal computer based training, or in person by the designated Privacy Officer, HIM Director or Security Officer.

Once the delivery format of the training programs is determined, the main issue with workforce education is keeping the content current and up to date with the fast changing regulations. Again, as with the automation of privacy and security monitoring and documentation, provision of 3rd party training materials is an increasing trend in order to facilitate compliance and reduce the burden associated with internal builds of privacy and security educational specific materials.
Mitigating Risk Associated with Privacy and Security

7. Public Relations / Consumer Confidence

Ultimately breaches or wrongful disclosure of PHI, along with any other types of published privacy or security violations will directly impact the standing of any healthcare organization within their community. This type of public relations challenge will be difficult to reverse given the public or consumer concern about keeping a sacred trust to protect their specific patient information or that of family members.

While we think of the consumer as strictly the patient and their family, we also know that the confidence of their associated healthcare professionals can also be shaken by such an event. Practicing physicians may not be comfortable continuing to refer their patients to a healthcare organization after breaches or publicized violations, which in the hyper competitive atmosphere of healthcare can have lasting and severe impacts to the organization’s reputation and bottom line.

Restoring faith in the healthcare provider and its workforce after such events requires a methodical approach to their mitigation and a track record of no further occurrences. Therefore, proactive steps should be taken to ensure that privacy and security compliance is tightened and more highly organized, with appropriate monitoring, documentation and reporting.

Since each Governing Board represents the community in which a healthcare organization is located, providing this group with updates about a breach is critical. As community stewards interfacing with the healthcare organization, the Governing Board and senior executives must be engaged to ensure the messaging of breach resolution and planned efforts to ensure that any future risk is eliminated.

Conclusion

Every healthcare organization regardless of size and complexity bears the responsibility and potential liability associated with meeting each federal and state mandate related to HIPAA privacy and security. The compliance demands and requirements of HIPAA privacy and security are but one area of requisite Compliance efforts and initiatives that are currently in progress. As a result of multiple, concurrent, enterprise and focused initiatives that each healthcare organization faces today, planning efforts become even more important so that valuable resources can be funded, coordinated, designated, supported and assigned the appropriate oversight. Given today’s numerous industry demands, we encourage each health
Mitigating Risk Associated with Privacy and Security

organization to invest time and effort to carefully plan these initiatives so that potential risks can be minimized or eliminated through processes, procedures, communications, oversight, and remediation tasks built into the initiative.

This white paper has highlighted seven areas of potential risk that might impact your HIPAA privacy and security efforts. While there can be other areas of risk as well, we believe that focusing on those areas with the most far-reaching impacts would serve as a checklist to compare each organization’s own internal planning for HIPAA privacy and security. Review these seven areas and augment the list to tailor it to your own healthcare environment.

1. Organizational Liability
2. Financial Impact / Cost
3. Processes to Detect, Inform and Escalate
4. Operational Efficiency
5. Technical Integrity
6. Employee and Physician Education
7. Public Relations / Consumer Confidence

We also encourage development of Contingency Plans as well since there may be situations in which an event may occur that is unforeseen in spite of careful planning, effective processes, diligent efforts and continued education of all staff and executives to safeguard against event.

Communicate often and continue to educate the entire organization, including the Board. There is no substitute for educating all professionals so that risks can be minimized or eliminated for the benefit of both the organization and members of the community who access healthcare services. Ultimately the trust of the community in the protection of their health information is an important linkage that must not and cannot be broken.

EHRs and other health IT will enhance the quality and value of health care, but only if there are appropriate protections in place to keep health information private and secure. Privacy and security are the bedrock of building trust, a must-have component that is essential to achieving meaningful use and realizing the value of health IT. Patients and providers must feel confident that laws, policies, and processes are in place to keep their health information private and secure, and that they will be enforced when violations occur.

Office of the National Coordinator for Health Information Technology (ONC)
Federal Health Information Technology Strategic Plan 2011 – 2015
About The Kiran Consortium Group LLC

The Kiran Consortium Group LLC (TKCG) is a professional services firm that provides experience and delivery excellence to our clients. We provide operational and information technology insights for the healthcare industry to accelerate processes introduce pragmatic solutions and share our knowledge with our clients. Our services include:

- Compliance,
- Implementation of Electronic Health Records,
- Interim Executive Services (e.g. Chief Executive Officers, Chief Information Officers, etc.), and
- Strategic Planning.

Given the enormous industry challenge to address HIPAA 5010 and ICD-10 Compliance while balancing Meaningful Use and HITECH/ARRA initiatives, TKCG has developed a toolkit to accelerate the assessment efforts. The U-Test-IT®, HIPAA 5010 and ICD-10 Toolkit, integrates a comprehensive Assessment, Work Plan, Issues Management, Governance, Contract Management, and Reporting functions to help clients to collect this baseline information and to identify potential risks and contingency plans to ensure Compliance success.

Contact Information: Info@Kiran-Consortium.com.

Guest Co-Author, Kelly McClendon, RHIA, CHPS

Mr. Kelly McClendon, RHIA, CHPS, is a Health Information Management professional with 30 years of industry experience with providers, vendors and consulting. He has expertise in HIPAA Privacy and Security and is a frequent industry speaker with many publications to date. His experience also includes product development to enhance provider productivity and efficiency. To contact Mr. McClendon, he can be reached at KMcClendon@xperts.com.

Other ICD-10 White Papers by Our Firm:

- **The C-Scape Series: A CEO’s Guide to Advancing ICD-10 Compliance Efforts** *(May, 2011)*
  A copy of this white paper is found on our website: [http://kiranconsortium.com/publications_index.html](http://kiranconsortium.com/publications_index.html).

  A copy of this white paper is found on our website: [http://kiranconsortium.com/publications_index.html](http://kiranconsortium.com/publications_index.html).

- **ICD-10: Data Impact Across the Enterprise** *(April, 2011)*
  Publication by the Healthcare Information Management and Systems Society (HIMSS) on a new web site, the *ICD-10 Playbook*, May 2011. For more information about the scheduled launch of the ICD-10 Playbook website, please visit the URL below for updates: [http://www.himss.org/asp/ContentRedirector.asp?ContentId=76859&cetID=200](http://www.himss.org/asp/ContentRedirector.asp?ContentId=76859&cetID=200).