FALL 2014 ▪ VOLUME 28 / NUMBER 4 ▪ www.himss.org

PRIVACY & SECURITY

Gerry Blass and Susan A. Miller, JD

Innovation in Healthcare

The Impact on Information Privacy & Security

Anyone who has worked in the healthcare industry over the past 30 years, including both authors, has seen tremendous advances in technology, including medical and informational advances, along with the impact of multi-organizational entities such as health information exchanges (HIEs) and accountable care organizations (ACOs). It seems to us that changes that began in the 1980s started slowly, then picked up steam in the 1990s, and are now moving ahead at a tremendous pace. Looking forward, we can't imagine what innovations are in store and how soon they will be here. And, we also can't imagine what new vulnerabilities to unauthorized access of protected health information (PHI) are also in store.

The Health Insurance Portability and Accountability Act (HIPAA) regulations are now almost 20 years old. Despite the Omnibus Rule updates in January 2013, the regulations have been fairly static. In fact, they were designed that way to be flexible enough to cover change, both within single covered entities (CEs) and business associates (BAs), and larger multi-organizational entities and the world of technologic advancement. The HIPAA Security rule is like a policy, broad in scope, and static. Therefore, each organization must also have detailed procedures that change along with organizational, administrative, physical, and technical changes.

It is hard to believe that the HIPAA Security Rule was written when most medical records were only in hardcopy format. There is still a large mix of hard copy and electronic medical records but that will soon all migrate to electronic format.

Today, HIPAA CEs and BAs must make sure they understand their current vulnerabilities that could impact how they protect PHI. We read about PHI breaches on a regular basis, and some have been huge. This kind of news has certainly caught the attention of healthcare leaders. The key is to continually have a program in place to access changes that result from innovation and try to stay one step ahead of related potential vulnerabilities.

Here are some areas to consider vulnerabilities and risk management in the healthcare world of today:

- Wireless
- Portable devices
- Virtual desktops
- HIEs
- Electronic health records (EHRs) and Meaningful Use (MU)
- ACOs
- Medical homes
- Governance
- Social media
- Mobile health
- Telemedicine
- Telecommuting
- Cloud storage and software
- Big data
- Breaches
- Cyber theft/Cyber insurance

Can we even imagine what areas are going to be added in the future? We can probably think it through and add some, but we can also guarantee our readers that the foregoing partial list is going to continually change at a rapid pace due to the continual innovations in healthcare.

So how can you handle rapid change due to innovations? Let's go back to the drawing board.

INFORMATION SECURITY RISK ANALYSIS AND ASSESSMENT

There is a reason why the MU rule for all stages requires an information security risk assessment. It makes sense that each stage

VISUAL PRIVACY PROTECTION used to mean turning over paper and moving a computer screen away from wandering eyes of patients or staff from a different area. Today all tablets and smart phones have cameras that can be used in to steal data and commit fraud.

will continue to introduce new innovation requirements. The bottom line is that CEs and BAs should conduct a risk assessment every year and have a change management process in place that requires a risk assessment whenever a new innovation is being implemented, in addition to regulation changes. And to be clear, we believe that the word "innovation" can be applied to changes that are organizational, administrative, physical, and technical. Wearable computers like Google Glass, iWatch, and more can introduce new vulnerabilities. Creating Big Data repositories and sharing them can introduce new vulnerabilities.

Previous columns by the authors have focused on the need for organizations to inventory ePHI in transit and at rest, and to then conduct a risk assessment to determine if current safeguards are adequate to reduce the risk of unauthorized access to an acceptable level. We suggest that this be a consistent periodic process that is discussed at information privacy and security governance meetings.

SENSITIVE DATA + VISUAL PRIVACY

Visual privacy protection used to mean turning over paper and moving a computer screen away from wandering eyes of patients or staff from a different area. Today all tablets and smart phones have cameras that can be used in to steal data and commit fraud. Consider all new innovations when conducting physical security audits, and make sure no PHI can be physically vulnerable to unauthorized access.

Here are some additional considerationss for physical security:

- Make sure your organization's policies and procedures include your staff working in public places, such as airports and on planes or trains, at conferences, or the library.
- Make sure your organization's workstation policies and procedures include all portable devices (USBs, smartphones, laptops, etc.)
- Make sure your organization's polices and procedures include dos and do nots for telecommuting and that they mesh with your organization's policies and procedures for working in public places.

ENCRYPTION

Encryption both for ePHI at rest and in transit is the current single best defense and is apt to continue to be for the foreseeable future for any CE and BA in today's world of constant technical change, such as workstations becoming tablets and smart phones, and social media and platforms in second and third generations, plus Big Data repositories.

BREACH RESPONSE TEAM AND FORENSICS AND THE CLOUD

Another defense measure is to have a breach response team and conduct tabletop tests for different scenarios that account for change management. Can you imagine doing forensics at your cloud vendor without a plan?

Your organization does not have access to your cloud vendor's servers, and you may not even know where they are. If your organization's ePHI is in a server offshore, let's imagine, how would your forensic expert or law enforcement obtain access to it?

In addition, your organization's ePHI could flow between and among multiple servers owned or leased by the cloud vendor and so you would need to document that and make sure those are assessed as well.

We suggest you use the National Institute of Standards and Technology (NIST) Cloud Computing Forensic Science Challenges document outlining 65 challenges and use them to update your organization's HIPAA

CE'S AND BA'S SHOULD conduct a risk assessment every year and have a change management process in place that requires a risk assessment whenever a new innovation is being implemented, in addition to regulation changes.

policies and procedures and breach plan and then roleplay scenarios. You can find the draft document here. We suggest you develop a cloud vendor breach checklist to use in case of such a breach.

TRAINING, TRAINING, TRAINING

As your organization adds and changes technology, participates in different payment plans, or is involved in social media, you will need to develop training on the privacy and security impacts of these to your organization and the new road map of updated policies, procedures, and other HIPAA documents.

CYBERSECURITY INSURANCE

Another way to mitigate risk is via cybersecurity insurance. It can even be used in paying a state or federal fine. Your organization's cybersecurity insurance should include a list of the areas your organization wants to cover, such as fines, notification, 800-line, and customer support. Plus, the authors suggest you ask the insurer if the coverage includes lost and stolen ePHI and e-tools, telecommuting, mobile tools, mobile health, telemedicine, cloud vendors, and other BAs, ACOs, medical homes, and other areas included in the previous list.

BUSINESS ASSOCIATE AGREEMENTS

BA Agreements (BAAs) are part of a CE or a BA's defense. First, they must be compliant with the Omnibus Rule, and be clear as to who has the responsibility for notification and payment of any fines. And your organization needs to know as well what privacy regulation permissions are the BA's in using and disclosing the CE's PHI and ePHI.

The BAA should state that first-level BAs must also execute agreements with their subcontractors and monitor them as well.

GOVERNANCE

Governance is the critical thing the Office of the National Coordinator (ONC) punted on when the industry replied a well heard "No More Regulations." ONC has created a framework and established several pilot programs that have yet to report.

Governance is usually defined as the rules of the road, the policies and procedures of an entity, and relates to the processes and decisions that define actions, grant power, and verify performance, within your organization and as your organization shares and receives ePHI.

In the multiple sharing environments such as an HIE, ACO, and others, governance requires a common set of behaviors, policies, and standards that enable exchange among all participants. This all has to do with interoperability! That is, the electronic exchange of ePHI in your local area, your state, and across the United States and its territories.

Because OCR punted, the weakest link in a security chain is still important to consider when you discuss, determine, and draft governance for the one-to-many data-sharing events that happen daily in all healthcare environments.

We suggest your organization know what it will accept and what it will not accept before it is asked to join an external organization such as an HIE, or when it is asked to share or accept ePHI from another healthcare entity.

MONITORING AND COMPLIANCE

All CEs and BAs should always be one step ahead of HIPAA Enforcement and Audits. The best way to achieve this is to have a monitoring and compliance program and updating the program as needed to keep up with all of the innovations ahead.

In reality, each area of HIPAA privacy and security should be included in every day discussions within CEs and BAs in the

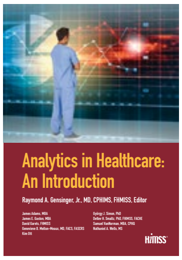
HIMSS Books

Read. Learn. Implement.

Save 20% when you purchase all three of these titles.

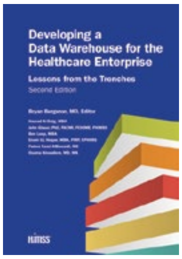
Data & Analytics Bundle

November 1-30


Analytics in Healthcare: An Introduction
Raymond A. Gensinger, Jr., MD, CPHIMS, FHIMSS, Editor
HIMSS

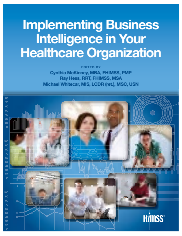
Analytics in Healthcare: An Introduction

A straightforward roadmap to achieving your goals within the domain of healthcare analytics, this book explores the evolution of healthcare analytics and tackles current challenges, including productive data mining from EHRs, data governance, and the DELTA analytics maturity model. An appendix with learning modules on secondary use of data and a comprehensive glossary are also included.


Developing a Data Warehouse for the Healthcare Enterprise
Lessons from the Trenches
Second Edition
HIMSS

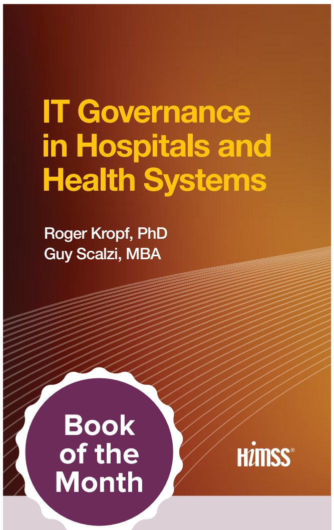
Developing a Data Warehouse for the Healthcare Enterprise: Lessons from the Trenches, 2nd Ed.

This follow up to the award-winning first edition offers guidance and multiple perspectives on the data warehouse development process—from the initial vision to system-wide release. Special features of the book include a sample RFP, data warehouse project plan, and information analysis template. A helpful glossary and acronyms list are also included.


Implementing Business Intelligence in Your Healthcare Organization
HIMSS

Implementing Business Intelligence in Your Healthcare Organization

This HIMSS Books best-seller offers an inside look at how healthcare organizations can use business intelligence to consistently monitor and improve upon patient outcomes, workload and costs. Through insightful chapters written by industry experts and numerous, real-world case studies, this book demonstrates myriad practical and proven steps to developing a business intelligence solution, including pre- and post-implementation issues.



20% off

IT Governance in Hospitals and Health Systems

HIMSS
transforming health through IT

For print books, visit:
himss.org/store

For eBooks, visit:
ebooks.himss.org

MAKE SURE YOUR organization's policies and procedures include your staff working in public places, like airports and on planes or trains, at conferences, or the library.

form of training, reminders, newsletters, screen saver messages, etc. Encourage your staff to think outside the box in every area and to bring suggestions and problems to designated privacy and security officers. Your workforce members are the eyes and ears and should be your first line of defense against unauthorized access of PHI.

In conclusion, your organization's HIPAA compliance must evolve and change as often as the healthcare environment within and outside your organization changes. Your HIPAA Privacy and Security compliance efforts must include a focus on innovations in healthcare. Remember, a foundational principal of your HIPAA privacy and security compliance should result in ongoing active defense against known vulnerabilities and for new ones that are byproducts of ongoing innovations in healthcare. **JHIM**

Gerry Blass is the President & CEO of ComplyAssistant. Blass has over 35 years of experience in healthcare IT and compliance. Blass provides IT and compliance consulting services and software (also called ComplyAssistant) that automates the management and documentation of healthcare compliance activities.
To learn more, visit www.complyassistant.com.

Susan A. Miller, JD, has 40 years of professional leadership experience spanning college teaching, biochemistry research, and law. Since 2002, Miller has provided independent consulting and legal services to numerous healthcare entities including NIST and HHS. She has co-authored two Office for Civil Rights (OCR) audit protocol prep-books, HIPAA Security Audit Prep Book, and HIPAA Breach & Privacy Audit Prep Book. You may reach her at TMSAM@aol.com. They are published here.
Blass and Miller are co-founders of HIPAA 411, a linked-in group.