Managing Information Privacy & Security in Healthcare

HIMSS Privacy and Security Toolkit Executive Summary
By Jeff Collman, PhD and Barbara Demster

Introduction
Ensuring a high and consistent level of privacy and security for health information both within and among individual healthcare organizations and throughout health information exchange (HIE) networks, requires those organizations entrusted with that healthcare information to establish formal information privacy and security programs with a strong governance infrastructure.

Managing healthcare information requires integrating good privacy and security business processes into the everyday working routines of all staff, not just implementing information technology privacy and security measures. The HIMSS Privacy and Security Toolkit outlines general principles and provides "best practice" examples of how healthcare providers should manage the privacy and security of their healthcare information, regardless of the medium in which it is maintained (paper, electronic, et.al). Sections of the Toolkit identify key activities from a variety of provider and business associate views that should be initiated as part of building a strong management program for information privacy and security. For a detailed history of the Toolkit, please see “History of the Privacy and Security Toolkit.”

HIMSS Privacy and Security Toolkit Background and Layout
In response to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Computer-based Patient Record Institute’s (CPRI) charter Work Group on Confidentiality, Privacy, and Security created the original “CPRI Security Toolkit” as a free resource to educate the healthcare industry on information technology security with the intent of assisting in the implementation of the new law. It was at a time when healthcare had not yet begun to embrace the electronic age on the clinical side of its business and the Internet was still in its infancy. The Toolkit has been updated and retooled over the ensuing years as technology advanced, and new regulations were released.

In 2010, the HIMSS Toolkit Work Group reorganized the contents and moved to a dashboard format that provides multiple avenues to access content. The updated Toolkit provides a format that makes it easier to access information by area of interest and contains new information relative to the latest regulatory requirements of the HITECH Act of 2009, new responsibilities of Health Information Exchanges (HIE) now designated as Business Associates, and other important advances in privacy and security.
The Toolkit update review of 2013 incorporated final regulations of the Omnibus Rule published in January 2013 which implements the HITECH Act, modifies the breach notification, privacy, security and enforcement rules and implements the underwriting nondiscrimination requirement of the Genetic Information Nondiscrimination Act (GINA).

The dashboard includes 11 major categories of organization. One document may be applicable to several categories and therefore accessible through exploration of each one. A list of Web sites and a glossary of terms appear at the end. The major categories are:

1. Introduction/Concepts: Basic Foundation Knowledge
2. Laws/Regulations: Local, state, federal, and international
4. Case Studies, Use Cases, Forms and Formats: Real world experiences
5. Personal Health Records: P&S issues unique to PHR
6. Policies & Procedures: Requirements and Samples
7. Privacy: All privacy related content
8. Executive Information: C-Suite considerations
9. Security: All security related content
10. Business Associates and Health Information Exchanges: Issues unique to BAs and HIEs
11. Specialty Segments: LTC, HHA, Physician Practices, Medical Devices among others

The new format resulted from extensive discussion about how best to represent the essential unity of health information privacy and security while acknowledging the practical need to distinguish them in practice from the particular perspective or view of the user. The expansion of categories reflects the variety of user perspectives required to implement a privacy and security program. The following provides a brief description of each category.

1. Introduction/Concepts: Basic Foundation Knowledge
   Basic information about a particular subject or area of the Toolkit. The intent is to provide a foundation of knowledge upon which to build.

2. Laws/Regulations: Local, state, federal, and international
   Materials directly related to local, state, federal, or international privacy and/or security laws or regulations.

   Provides information from a variety of and views on what the industry considers to be accepted practices and procedures for optimal outcomes. These may be high level or very detailed procedures developed by professional associations utilizing experts in the field.

4. Case Studies, Use Cases, Forms and Formats: Real world experiences
   Reports of real world experiences used to describe factors that contribute to the success or failure of real organizations. Case Studies may be a model to emulate or a model that details pitfalls to avoid. Use cases describe how the world interacts with a system and the necessary functional requirements for
accomplishing a required outcome. Forms and Formats provide real examples of tools used in the named healthcare organizations contributing to the Toolkit.

5. **Personal Health Records: P&S issues unique to PHR**
   This section provides information relevant to Personal Health Records. It includes information needed to understand the P&S environment surrounding and necessary to support a PHR.

6. **Policies & Procedures: Requirements and Samples**
   This section focuses on the Policies and Procedures required for effective P&S programs. Examples of actual P&Ps are included as well as discussion of regulatory requirements for P&Ps and their content.

7. **Privacy: All privacy related content**
   This identifies all materials that deal with privacy of health information issues. Some materials may overlap with security concerns but not necessarily.

8. **Executive Information: C-Suite considerations**
   Identifies material that will inform executive decision making in the areas of privacy and security.

9. **Security: All security related content**
   Identifies all materials that deal with security issues. There may be some overlap with privacy but not necessarily.

10. **Business Associates and Health Information Exchanges: Issues unique to BAs and HIEs**
    Materials that address the unique needs of the Health Information Exchange and the Business Associate in the areas of privacy and security.

11. **Specialty Segments: LTC, HHA, Physician Practices, Medical Devices among others**
    This section groups information that deals with distinct recognized segments of the healthcare industry that have unique requirements in P&S. Examples are LTC, Home Health, Physician Practices, Medical Devices, among others.

**Feedback from Toolkit users**
The new format provides for a feedback capability to the HIMSS Privacy and Security Content Review Task Force. Please use this feature to provide suggestions for new content as well as any comments to the Task Force for consideration.

**Additional Privacy & Security Toolkits**
Over the years, the HIMSS Privacy and Security Toolkit has spawned additional Toolkits that address subspecialty areas of security that have their own in-depth body of knowledge. These toolkits (listed below) can be found at http://www.himss.org/library/healthcare-privacy-security?navItemNumber=13400.

- Privacy and Security Toolkit for Small Provider Organizations
- Patient Identity Integrity Toolkit
D01 – Executive Summary

- Risk Assessment Toolkit
- Mobile Security Toolkit
- Cloud Security Toolkit