



## Managing Information Privacy & Security in Healthcare

### HIMSS Privacy and Security Toolkit Executive Summary

By Jeff Collman, PhD

#### Introduction

Ensuring a high and consistent level of information security for electronic health records (EHRs, both within individual healthcare organizations and throughout the entire healthcare delivery system, requires organizations entrusted with healthcare information to establish formal information security programs.

HIMSS believes that managing healthcare information requires integrating good security processes into the everyday working routines of all staff, not just implementing information technology security measures. The Toolkit outlines general principles and provides "best practice" examples of how healthcare providers should manage the security of their paper and electronic records. The sections of the Toolkit identify key activities that healthcare providers should initiate as part of managing information security.

#### History of the Toolkit

Recognizing the importance of information security in managing computer-based patient records, the Computer-based Patient Record Institute (CPRI) chartered the Work Group on Confidentiality, Privacy, and Security in 1993. For three years, the Work Group developed and published a series of topical booklets providing guidelines for improving information security for organizations implementing EHRs. The guideline series addressed separate issues in information security, but, taken as a whole, promoted a comprehensive organizational process. With the emergence of HIPAA in 1996, CPRI decided to consolidate and expand this initial series into a single, comprehensive reference. Thus was born the *CPRI Toolkit: Managing Information Security in Healthcare*. The CPRI Toolkit Workgroup committed itself to preparing regular updates as the field of health information security developed and produced Versions 1, 2 and 3 under the auspices of CPRI. Version 3 was a particularly important update because it added extensive new material on the recently published final HIPAA security rule. In 2002, the CPRI merged with the Health Information and Management Systems Society (HIMSS) bringing along the Toolkit with its Workgroup.

HIMSS has sponsored three updates of the Toolkit, Versions 4, 5 and now 6. Version 5 marked another milestone in the development of the Toolkit with the addition of a large section with many new chapters devoted entirely to health information privacy. Version 5 also attempted to exploit the power of the World Wide Web to offer links to many online resources. With Version 6, the Toolkit acquires several new chapters including a new section on security in the emerging national health information network and

similar vast architectures, a completely new organization and a new name, the *HIMSS Privacy and Security Toolkit*. All existing chapters were reviewed and, when appropriate, updated. With the HIMSS Toolkit, a healthcare organization should be able to plan, implement, and evaluate privacy and security surveillance processes scaled to their organizational needs. These resources should aid healthcare organizations in securely managing information, particularly as they develop responses to new federal regulations and laws such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 or the Federal Information Security Management Act (FISMA) of 2002.

### **HIMSS Privacy and Security Toolkit Layout**

The HIMSS Toolkit now includes five major sections with multiple chapters under each section as well as a consolidated annotated bibliography. A list of Web sites and a glossary of terms appear at the end. The major sections are:

- Privacy and Security principles
- Rights & Obligations – Laws, Regulations & Standards
- Policies
- Practices
- Case Studies

The new layout resulted from an 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. Thus, the HIMSS Toolkit flows from general principles to specific case studies. We observe the unity of health information privacy and security at both ends of the spectrum in principles and in practice as illustrated in the case studies. We recognize their divergence in laws, regulations and standards as well as specific policies and practices.

### **Privacy and Security Principles**

This section of the HIMSS Toolkit asks a basic question: “What principles should guide our understanding of the privacy and security of health information?” Each chapter attempts addresses the basic principles of privacy and security from the perspective of specific audiences. The opening chapter for all audiences explains the historical roots as well as some contemporary updates of health information privacy and security principles. “A Primer in Health Information Security” explains basic concepts in privacy and security for individuals just beginning to learn about health data security. The white paper for executives highlights concerns that require the sustained attention of senior leadership in healthcare organizations. The final chapter of this section explains the joint approach to protecting health information of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and the National Committee for Quality Assurance (NCQA).

### **Rights & Obligations – Laws, Regulations & Standards**

Currently, questions of health information security and medical privacy are of utmost importance in the United States. Hardly a day goes by that *The Washington Post*, *The New York Times* or *USA Today* do not feature an article about some aspect of medical privacy or security. Opinion polls document that the American public regards the data management practices of most large organizations with great skepticism. In partial response to these and other expressions of public concern, President Clinton commissioned a task force on medical privacy as part of his healthcare reform efforts. Although the recommendations of the privacy task force died along with Clinton’s plan, federal legislators have incorporated some of their intent,

particularly the requirement of federal medical privacy legislation, into subsequent approaches to healthcare reform. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created specific requirements for the Congress and HHS. Because of HIPAA, the legal and regulatory environment for managing patient medical information has dramatically changed. HHS has developed regulations for managing health information privacy and security. In Version 6 of the *HIMSS Toolkit*, we expand our coverage of regulatory issues by material on new federal laws such as FISMA and Gramm-Leach-Bliley as well as expanding existing material on international regulations.

## **Policies**

Changes in the regulatory and legal environments, the security risks of distributed networks and systems, ever-changing information technology, and rising patient expectations all require healthcare organizations to continuously update their data security policies, procedures, and practices. A security team must take primary responsibility for coordinating this effort through careful risk analysis, security policy review, and technical and operational enhancements. The security team's efforts will fail, however, without strong business and clinical leadership from throughout the organization. Even if key leaders accept responsibility for maintaining the confidentiality of patient identifiable information, staff will often resist taking on new tasks that further complicate their work and compete with current tasks. The security team must recognize that enhancing the organization's security capability requires transforming institutional resistance into a mission-based mobilized security effort. A security team that neglects building support for its efforts risks failure.

Included in the *HIMSS Toolkit* are sample documents illustrating approaches to privacy and security policies, security risk analyses, patient consent and disclosure authorization documents, and other issues from several organizations, including the American Health Information Management Association, Beth Israel Deaconess Medical Center, Kaiser Permanente of Northern California, Partners HealthCare System Inc., Mayo Foundation, Harvard Vanguard Medical Associates, and several NLM-funded sites. These examples should assist any healthcare program, large or small, in efforts to enhance the security of its confidential information.

## **Practices**

This section of the *HIMSS Toolkit*, Version 6 addresses many of the "nuts-and-bolts" of health information privacy and security. Major subheadings include Health Information Risk Assessment & Management, Business Continuity Planning & Disaster Recovery Planning, Organizing Privacy and Security Training, Enforcing Security Policy, Enhancing Patient Understanding, Institutionalizing Responsibility and Health Network Infrastructure. For example, under the subheading of Enhancing Patient Understanding, a chapter appears about the personal health record (PHR). It provides guidance for thinking about the PHR, including a special section on probing PHR controls for privacy and security. The new section, Health Information Infrastructure, includes several specially commissioned chapters on various dimensions of privacy and security in the emerging national and global health networks such as the National Health Information Network, the defense Global Grid and the Public Health Network.

### **Case Studies**

This section includes special case studies of broad interest. A new chapter explains the special efforts of the Social Security Administration to protect client information in its automated claims management system, a topic of vital interest to care providers and Medicare beneficiaries.

### **Future releases**

The HIMSS Privacy and Security Toolkit Workgroup has adopted a quarterly update schedule. Several more new chapters are planned for the next release in April 2007. Please forward suggestions for new chapters and comments to Lisa Gallagher at [lgallagher@himss.org](mailto:lgallagher@himss.org).