

INFORMATION SECURITY IN HEALTHCARE: MANAGING RISK

Terrell Herzig, MSHI, CISSP



Information Security in Healthcare

Managing Risk

Edited by
Terrell W. Herzig, MSHI, CISSP



HIMSS Mission

To lead healthcare transformation through effective use of health information technology.

© 2010 by Healthcare Information and Management Systems Society (HIMSS).
All rights reserved. No part of this publication may be reproduced, adapted, translated, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Printed in the U.S.A. 5 4 3 2 1

Requests for permission to make copies of any part of this work should be sent to:

Permissions Editor

HIMSS

230 E. Ohio, Suite 500

Chicago, IL 60611-3269

mschlossberg@himss.org

The inclusion of an organization name, product or service in this publication should not be considered as an endorsement of such organization, product or service, nor is the failure to include an organization name, product or service to be construed as disapproval.

ISBN 978-0-9821070-2-7

For more information about HIMSS, please visit www.himss.org.

About the Editor

Terrell W. Herzig, MSHI, CISSP, is Information Security Officer of the UAB Health System, Birmingham, Alabama, the UAB HIPAA Security Officer, and an Adjunct Professor of Health Informatics at the University of Alabama at Birmingham (UAB). Mr. Herzig teaches graduate courses in Information Engineering, Programming, Computer Networks and Information Security in the UAB School of Health Professions. During his tenure at UAB, he has served as Director of Information Technology for the Civitan International Research Center and Director of Informatics for the Pittman General Clinical Research Center. Mr. Herzig has also consulted on numerous informatics projects with external groups, including Southern Nuclear and the US Army Medical Command.

About the Contributors

Mary Anne S. Canant, MBA, CISA, CISSP, is a Senior Information Systems Auditor at the University of Alabama (UA), Tuscaloosa, for which she provides assurance and advisory services. Her current interests include risk, control and governance of information technologies, and assets supporting UA's Academic Health Center and research enterprise.

Leanne Cordisco, BMET, BS, is the Healthcare IT Program Manager for GE Healthcare. Ms. Cordisco combines 21 years of experience in biomedical engineering with seven years' experience in IT. She works to advance the field of clinical engineering through the development of healthcare IT technical training programs. Ms. Cordisco is a member of the American College of Clinical Engineering, the American Society for Training and Development, and HIMSS. She has authored or presented on more than 20 different healthcare IT-related topics.

Brian Evans, CISSP, CISM, serves as President of Brian Evans Consulting and provides information risk management consultation for clients throughout the United States. He held a similar role as the Principal Risk Strategist for Cardinal Health. Mr. Evans led the Enterprise Computer Incident Response and Forensic Investigations teams for Nationwide Insurance and served as Vice President of Corporate Information Security at Key Bank. As the National Delivery Director and Senior Security Consultant for Computer Task Group, he directed clients on building effective compliance and information risk management programs. Mr. Evans served as Information Security Officer at The Ohio State University Health System and has held positions at the Ohio Department of Health. He also managed Incident Response and Recovery teams in the US Air Force. Mr. Evans earned a master's degree in Public Administration from the University of Cincinnati, Ohio, and a Bachelor of Science degree in Business Management from the University of Maryland, College Park.

Sharon Finney is the Corporate Data Security Officer for Adventist Health System, the largest not-for-profit, Protestant healthcare system in the United States. Adventist Health System currently operates 37 hospitals, 17 skilled nursing facilities, and more than 20 home health, hospice, medical equipment, and infusion entities in 10 states. Ms. Finney is responsible for the data security technology and compliance strategies and data security operations for Adventist Health System. She has more than 20 years of experience in information technology and data security and holds a Bachelor of Science degree in Business Administration.

J. David Kirby, MS, CISSP, CHPS, has served, for more than 30 years, in various roles, developing innovative uses of health information technology with a variety of public, private, state, national, and international organizations. These roles include academic medical center (AMC) information security officer, director of an AMC-based telehealth program, director of an IT innovation center in an AMC, and manager of technology support for an AMC. As current President of Kirby Information Management Consulting LLC (KirbyIMC.com), he provides consulting in innovative health information technology, security, and privacy areas. Customers include healthcare enterprises and information technology vendors of all sizes and types. Mr. Kirby holds Bachelor of Science and Master of Science degrees in Computer Science and certificates in security and privacy, including CISSP, CHPS, and CHS. He is an Adjunct Associate Professor in the Division of Medical Informatics at Duke University Medical Center, Durham, NC.

Mac McMillan is cofounder and CEO of CynergisTek, Inc., a firm specializing in information security, regulatory compliance, and IT audit. Mr. McMillan brings 30 years of security countermeasures experience to his philosophy of managing security programs. He has worked in the healthcare industry since 2000 and frequently contributes to HCCA, AHIA, AHIMA, AHLA, and HIMSS programs. He currently serves as chair for HIMSS' Information Systems Security Work Group. He served as Director of Security for two Department of Defense agencies, receiving both the Silver and Gold Medals for Exceptional Meritorious Service. He holds a Master of Arts degree in National Security and Strategic Studies from the US Naval War College; and a Bachelor of Science degree in Education from Texas A&M University. He was a 1993-1994 Excellence in Government Fellow and is a graduate of the Senior Officials in National Security program from the John F. Kennedy School of Government, Harvard University.

Shelia T. Searson, CIPP, is Program Director in the University of Alabama at Birmingham's (UAB) HIPAA Office. In this role, she has the unique opportunity of working with both the UAB academic units that fall under the HIPAA regulations and the UAB Health System components. Ms. Searson is a member of a UAB team that reports to the UAB Privacy Office and works to ensure compliance with HIPAA privacy and security regulations. Ms. Searson holds a baccalaureate degree in Speech Communications from Shorter College in Rome, Georgia. Her professional affiliations include the International Association of Privacy Professionals, through which she is a Certified Information Privacy Professional, and the American Health Information Management Association.

Tom Walsh, CISSP, is a Certified Information Systems Security Professional (CISSP) and a nationally recognized speaker. As an independent consultant, Tom conducts security training, risk analysis, business impact analysis, business continuity, and disaster recovery planning for clients. Mr. Walsh is also the coauthor of two books, *Medical Records Disaster Planning—A Health Information Manager's Survival Guide* (American Health Information Management Association, 2008) and *Handbook for HIPAA Security Implementation* (American Medical Association, 2003).

Lory Wood is President of Compiled Logic Wares Consulting. As CIO/CSO of Good Health Network (GHN), she deployed a standards-based, secure PKI-enabled Web-based personal health record that is patient owned and controlled and is HIPAA-compliant. GHN is a healthcare certification authority. Ms. Wood is a member of the HITSP Consumer Perspective, Security Privacy and Infrastructure Technical Committee; the Education Communications Outreach Committee; ASTM E31 Healthcare Informatics Committees, including the Continuity of Care Record Technical Workgroup; PDF Healthcare Workgroup; vice chair of HIMSS' PHR Steering Committee; and co-chair of the CCHIT PHR workgroup. She is also Project Manager for the Florida Medicaid Pharmacology Project, which deploys 1,500 PDA/smart phones to physicians serving Medicaid patients. Ms. Wood was lead engineer for DOD T2P2 telemedicine browser-based eConsultation, utilizing secure satellite technology across the Pacific Rim and was awarded the 1999 Technology Excellence in Government Award.

Contents

| | |
|--|-------------|
| Preface | xi |
| Introduction | xiii |
| <i>Shelia T. Searson, CIPP</i> | |
| Chapter 1: IT Security Governance | 1 |
| <i>Mac McMillan</i> | |
| Chapter 2: Risk Management and Strategic Planning | 9 |
| <i>Tom Walsh, CISSP</i> | |
| Chapter 3: Data Management and Portability | 27 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 4: Audit Logging | 45 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 5: Identity and Access Management | 55 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 6: Sharing Patient Information | 75 |
| <i>J. David Kirby, BS, MS, CISSP, CHPS</i> | |
| Chapter 7: Portable Devices | 95 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 8: Medical Device Security Implications | 113 |
| <i>Leanne Cordisco, BMET, BS</i> | |
| Chapter 9: Remote Access | 125 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 10: Training the Workforce | 141 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 11: The Importance of Incident Response | 151 |
| <i>Brian Evans, CISSP, CISM</i> | |
| Chapter 12: Disaster Recovery and Business Continuity | 171 |
| <i>Tom Walsh, CISSP</i> | |
| Chapter 13: Developing an Effective Compliance Strategy | 195 |
| <i>Sharon Finney</i> | |
| Chapter 14: Managing Security with Outsourcing Partners | 205 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 15: Physical Security | 217 |
| <i>Terrell W. Herzig, MSHI, CISSP</i> | |
| Chapter 16: Effective Security Programs Enable Clinical and Business Improvements | 237 |
| <i>Mary Anne S. Canant, MBA, CISA, CISSP</i> | |
| Chapter 17: The Foundations of Information Assurance | 247 |
| <i>Mary Anne S. Canant, MBA, CISA, CISSP</i> | |
| Chapter 18: Personal Health Records | 255 |
| <i>Lory Wood</i> | |
| Appendix A: Resources for Information Privacy and Security in Healthcare | 273 |
| Appendix B: Sample Security Plan | 289 |

Preface

Terrell W. Herzig, MSHI, CISSP

It seems like almost every day you read an article regarding the loss of a laptop or a security breach resulting in the loss of patient information. In February of 2009, President Obama signed into law the American Recovery and Reinvestment Act, in effect, creating the first federal breach law. The industry impacted by this law—healthcare. Indeed, ask anyone on the street to list what information about them would be considered the most sensitive if it were publically released, and they would probably answer medical information.

Healthcare presents many unique challenges to information security professionals. First, information must not only be kept confidential, but must be extremely accurate and always available. Second, defining the type and level of access is difficult. Indeed, many people must have access to medical information in order not to impede patient care.

Organizations must use the information they collect to fine-tune operations and cut costs. As the industry embraces new technologies to network and share patient information, it too must secure and guard access to highly sensitive data. Understanding the issues involved can help guide IT expenditures, enable competitive advantages and avoid costly regulatory fines and penalties.

A lot of good information security books are available on the market. Most of these books deal with information security at a low technical level. The intent of this book is to present information security—unique to the healthcare environment—from multiple viewpoints. First, the book is intended to be informative and educational for healthcare managers. From board-level senior managers to front-line management, the book is intended to present healthcare information security practices and concerns in straight-forward language. Second, for practicing information security professionals, the intent is to help them tweak or jump start an appropriate information security management program. Last, but not least, the book should appeal to college education and training programs for healthcare environments.

This book combines the experience and insight of several healthcare IT managers and information security professionals to bring important privacy and security issues to life. Many thanks to each one for providing the readers with tools, checklists, and content to help them build and/or enhance their information security activities. One thing is certain: In this ever-changing information security environment, everyone involved with maintaining privacy and security of healthcare data need continuing support, encouragement, and guidance to remain current and informed. I trust this book will meet some of those needs and provide new and renewed insight into information security as it pertains to healthcare.

Introduction

Shelia T. Searson, CIPP

Why introduce a security book by beginning with a discussion about privacy? A very good question. Privacy should be a critical component of any healthcare institution's strategic vision or operational plan. Most individuals, especially citizens of the United States, assume they have a right to privacy—the right to control the events in their personal lives and the right to keep their personal information secret if they so choose.¹ However, the word *privacy* is not actually included in the Constitution of the United States.²

Even so, the right to privacy is viewed as an important component of one's personal freedom, and there is no place that this right is held with stronger conviction than in the relationship between healthcare institutions and patients' personal health information.³

Privacy, although not well-defined, is generally understood as the appropriate use of personal information in a range of circumstances. The International Association of Privacy Professionals adds that “what is appropriate will depend on context, law, and the individual's expectations.”⁴ For our purposes, the terms *privacy* and *information privacy* are synonymous.

Information privacy means that an individual has control of his or her personal information and has reasonable expectations about how this personal information will be used and when it may be disclosed to others.⁵ Individuals are sensitive and protective of their personal information, which is generally thought to include address, birth date and age, Social Security number, credit card numbers, salary and debt, and medical conditions. The right to privacy includes the precept that this information will be kept private, confidential and secure.

Depending on a particular situation or environment, an individual may choose to disclose personal information, but this is an individual choice, not an organizational decision. When an individual grants permission for others to use his or her personal information for a specific purpose, that permission includes an expectation that the information, which is private and confidential, will be used only as specified or approved by that individual.

The appropriate use of confidential information is dependent on various privacy laws and regulations that affect such areas as workplace privacy, healthcare, student records and financial information. Each institution must determine those federal laws and sets of regulations with which they are required to comply.

For a healthcare institution, personal information could include patient medical records, employee records, credit or debit card numbers, research data, and passwords

or other means of access to its information systems. In the case of an academic health center, add student records to the mix of personal information that must be kept private, confidential and secure.

Healthcare institutions are involved in a careful balance of an individual's privacy rights and the use of the confidential information to perform necessary clinical or business tasks. These tasks have a variety of purposes, ranging from personnel issues related to payroll and benefits to providing direct clinical care, performing laboratory tests, prescribing medications and sharing results with referring physicians. Protecting the privacy of all constituencies within a healthcare institution, including employees, patients, healthcare providers and volunteers, can be a daunting, but reasonable privacy expectation in the current litigious environment. For our purposes, the focus of this book is on personal and health information of patients.

The most encompassing privacy law affecting healthcare institutions is the federal Health Insurance Portability and Accountability Act of 1996, better known as HIPAA. Before HIPAA, the privacy and confidentiality of a patient's health information involved a patchwork of federal and state laws and regulations, professional codes of ethics, standards of practice, and the policies of individual institutions.⁶

Examples of federal regulations affecting healthcare are the Privacy Act and the Federal Policy for the Protection of Human Subjects. The Privacy Act of 1974 was enacted because of concerns related to government misuse of citizen information contained in computerized databases. The act only applies to federal government entities and federal contractors as they use the identifiable personal information of US citizens and legal residents. Therefore, it only regulates healthcare institutions that are federally operated or funded.⁷

The Federal Policy for the Protection of Human Subjects, most usually referred to as the Common Rule, is a set of privacy regulations overseeing federally funded clinical trials and medical research protocols involving human subjects. The Common Rule requires sufficient protection for the privacy of research participants and the confidentiality of the research data. However, the policy relates only to those research projects that are federally funded.⁷

HIPAA provides a broad definition and scope regarding a patient's health information, which HIPAA refers to as protected health information (PHI). PHI includes all oral, written, and electronically maintained information that is created or received by a healthcare provider, a health plan, or a healthcare clearinghouse. PHI includes that information related to an individual's past, present, or future physical or mental health condition or the past, present or future payment for the provision of healthcare.⁷

In essence, PHI is not the actual health or medical record of a patient but rather those data elements that can be used to identify a person when linked with that person's medical information, such as a medical diagnosis or medical condition. PHI data elements, as outlined in HIPAA, include 18 identifiers:

- Names

- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and equivalent geocodes
- All elements of dates (except year) directly related to an individual, including date of birth, admission and discharge dates, date of death, and all ages older than 89 years, as well as all elements of dates (including year) indicative of such age
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security number
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification (164.514(c)).¹²

Many of these identifiers are included as necessary measures to ensure patient privacy protections. Name, address, Social Security number, birth date, and account numbers are logical pieces of information to keep private and secure, as these data can easily identify an individual.

However, it may not be immediately evident why certain other data elements are included. Could the serial number or license plate number from an individual's vehicle be used to identify that individual? Why include the serial number from a pacemaker implanted into a cardiovascular patient or from surgical steel used to set a patient's broken ankle? In fact such data elements represent small puzzle pieces that could be investigated and added to other information to identify a patient.

Using or maintaining PHI is not to be confused with using or maintaining a patient's medical record. The data being used or stored must be reviewed in light of these 18 PHI data elements. One of the data elements listed, combined with a medical condition or diagnosis, represents PHI that is protected under HIPAA privacy regulations. For example, information from a database entitled "Former Patients with Lymphoma" (reference to a diagnosis) that includes the patients' names (PHI data element) is considered PHI. Therefore, patient information in clinical and research databases must be used and disclosed in a manner consistent with the HIPAA Privacy Rule.⁸

Healthcare institutions must also comply with state privacy laws and regulations. Of course, these requirements vary greatly from state to state, and HIPAA's privacy protections provide a federal "floor" on which state privacy laws can build.⁷ However, the HIPAA Privacy Rule pre-empts state law when the state law is contrary to the Privacy Rule. However, as with most federal regulations, there are exceptions to HIPAA's pre-emption. A common exception is when state law is more stringent than the Privacy Rule in protecting the privacy of PHI.³ HIPAA represents the floor, or minimum of privacy protections, and allows greater protection provided by the states.

Recent legislation, the American Recovery and Reinvestment Act of 2009 (ARRA), better known as "the Stimulus Bill," signed into federal law on February 17, 2009, significantly enhances and strengthens privacy and security regulations contained in HIPAA.⁹ ARRA includes the Health Information Technology for Economic and Clinical Health Act, or the HITECH Act.¹⁰ The HITECH Act promotes the use of health information technology (HIT) and specifically extends the legal provisions of the HIPAA privacy and security regulations. HIPAA-covered entities, business associates of covered entities, and some entities previously not considered to be HIPAA-covered entities are affected by these new requirements.⁹ The HITECH Act establishes breach notification requirements, further limits the uses and disclosures of PHI, and increases the enforcement of, and the penalties for, noncompliance with HIPAA privacy and security regulations. These requirements represent efforts to keep pace with the new risks to PHI that have emerged since the enactment of HIPAA in 1996. Many HITECH provisions are effective within the first 12 months, while other pieces of the legislation go into effect at later dates.¹⁰ Additional guidance and interpretation regarding the provisions in the law are anticipated, and careful consideration should be given to these emerging regulatory requirements.

So, why is privacy included in any serious consideration of information security? Actually, HIPAA provides regulations to protect both the privacy and security of PHI received and maintained by healthcare institutions. HIPAA's Privacy Rule sets forth regulatory standards for the use and disclosure of PHI, and the Security Regulations, comprised of 18 standards, ensure the confidentiality, integrity, and availability of PHI for business-related purposes.⁴

By definition, *information security* refers to protecting information against loss, unauthorized access, or misuse. It includes assessing the threats and risks to information and assuring confidentiality, integrity, and availability of the data being protected.¹ Therefore, although information privacy and information security are different in concept, they are related in practice. Privacy depends on information security, especially for the confidentiality of the information being protected.⁵

Privacy and security work together in a complementary fashion. For example, strong privacy policies and procedures are worthless if outsiders can break into the institution's information systems and compromise or steal the data. Therefore, privacy and security share a common goal of preventing the unauthorized access, use, and release of confidential information. Sound security practices create audit trails to determine who has accessed confidential, sensitive, or personal information. These audit trails provide the means to encourage adherence to privacy and information

security policies and standards and to discourage wrongdoing by enforcing disciplinary actions for misconduct. Both the privacy and security provided to the sensitive data are strengthened.¹¹

However, HIPAA privacy and security regulations represent the minimum standards of protection on which management can build policies and practices that are reasonable and appropriate for their institution.⁷ The HIPAA privacy and security regulations provide sound minimal guidelines to be followed for the protection of all sensitive or confidential data, not just PHI. An institution's privacy and information security policies and procedures must strike a balance between ensuring privacy for personal and confidential data and permitting important intended business uses of the information.

Once the policies are developed, they must be implemented and enforced. Individual leaders and managers in a healthcare organization must emphasize and reward the importance of privacy and support the interrelationship of privacy and information security. Neither privacy nor information security can exist in a vacuum. Privacy is necessary for today's information-driven, technologically advanced environment. Information security can provide the "privacy" assurance that information technology needs. Administration must strongly support this marriage of privacy and information security, making both important priorities for the institution.

The healthcare workforce needs to know what information is to be kept confidential and the manner in which this is to be accomplished. Knowledge of the institution's policies and operating procedures and understanding business needs and access to the appropriate information are essential at all levels. Formal training about an institution's privacy and information security policies and procedures is an important component of an effective compliance program.

The adage that says "you can have security without privacy, but you cannot have privacy without security"¹ effectively denotes the relationship between information privacy and information security and serves as the rationale for including privacy in any serious consideration of information security. Privacy is the appropriate use of information, and security is the protection of that information while it is being used.¹ The two are explicitly intertwined.¹³ The following chapters provide a complete assessment of information security principles and their essential role in protecting privacy and confidentiality of sensitive institutional assets such as PHI.

References

1. International Association of Privacy Professionals. *Information Privacy Certification Training Course Book*, York, Me: IAPP; 2006.
2. Alderman E, Kennedy C. *The Right to Privacy*. New York, NY: Vintage; 1997; xiii.
3. American Health Information Management Association. *HIPAA in Practice*. Chicago, Ill: AHIMA; 2004; vii.
4. International Association of Privacy Professionals. *IAPP Information Privacy Certification Glossary of Common Privacy Terminology*. York, Me: IAPP; 2006.
5. Borten K. *The No-Hassle Guide to HIPAA Policies*. Marblehead, Mass: HCPro; 2007.

6. Hughes G. Laws and Regulations Governing the Disclosure of Health Information (AHIMA Practice Brief). Updated November 2002. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_016464.hcsp?dDocName=bok1_016464.
7. Boyle L, Mack D. *HIPAA: A Guide to Health Care Privacy and Security Law*. Frederick, Md: Aspen; 2009.
8. Searson S, Hicks J, Cole J, Herzig T, Brooks CM. HIPAA for cancer educators. Accepted for publication by the *Journal of Cancer Education*.
9. American Health Information Management Association. Analysis of Health Care Confidentiality, Privacy, and Security Provisions of The American Recovery and Reinvestment Act of 2009, Public Law 111-5. March 2009.
10. Hirsch R, Fayed R. ARRA 2009 and the HITECH Act: The next phase of HIPAA regulation and enforcement arrives. *The Bureau of National Affairs' Health Law Reporter*, 2009.
11. Swire P, Steinfeld L. Security and Privacy After September 11: The Health Care Example. Copyright held by author/owner. 4. <http://www.cfp2002.org/proceedings/proceedings/swire.pdf>
12. Department of Health and Human Services. Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule.
13. Sealet S. Without security there can be no privacy. November 1, 2001. Available at: <http://www.cio.com/article/print30639>.