



## Managing Information Privacy & Security in Healthcare

### HIMSS Sound Security Practices

By the HIMSS Privacy and Security Task Force

The Sound Security Practices is a reference document compiled and published by the HIMSS Privacy and Security Task Force. It is intended for the use of HIMSS members, providers and payers. It identifies resources such as standards and guidelines that are well established. The security practices are grouped under three major categories namely, standards organizations, government agencies and others such as trade associations, think tanks, security practitioners, etc. HIMSS members and organizations that are involved in creating, managing, implementing information security policies and procedures can use this document as a resource guide. It can be used as an easy reference both for education and implementation support. The format of Sound Security Practices and Sound Privacy Practices are kept the same as they are intended for the same audience.

#### *Standards Organizations*

##### ***1. American Society for Testing and Materials (ASTM)***

ASTM is one of the world's oldest and largest standards development organizations.

##### **Committee E31 Healthcare Informatics**

<http://www.astm.org/>

This committee maintains a number of useful guides and standards.

E1869-97 Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records

E1986-98 Standard Guide for Information Access Privileges to Health Information

E1987-98 Standard Guide for Individual Rights Regarding Health Information

E1988-98 Standard Guide for Training of Persons who have Access to Health Information

E2017-99 Standard Guide for Amendments to Health Information

E2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems

E1714-00 Standard Guide for Properties of a Universal Healthcare Identifier (UHID)

E1762-95 Standard Guide for Electronic Authentication of Health Care Information

E1985-98 Standard Guide for User Authentication and Authorization

E2084-00 Standard Specification for Authentication of Healthcare Information Using Digital Signatures

E2085-00a Standard Guide on Security Framework for Healthcare Information

E2086-00 Standard Guide for Internet and Intranet Healthcare Security

E2212-02a Standard Practice Healthcare Certificate Policy

E1902-02 Standard Guide for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records

## ***2. International Standards Organization (ISO)***

"Code of Practices for Information Technology Management" (ISO 17799) is an adaptation of BS 7799 Part 1. Both spell out general guidelines for good information security, but ISO didn't incorporate the certification component--Part 2 of the British standard.

## ***3. ISO 13335***

This guideline defines a variety of security controls and outlines the framework for risk management. However, like ISO 17799, it doesn't specify the means for implementing security measures.

## ***4. ISO 15408/Common Criteria***

This standard provides the framework for testing the effectiveness of most security systems and individual security solutions. However, it isn't intended to measure the effectiveness of an organization's overall security program.

## ***Government Agencies***

### ***5. Department of Homeland Security Information Analysis & Infrastructure Protection (IAIP) Office***

<http://www.dhs.gov/dhspublic/display?theme=52>

The Critical Infrastructure Assurance Office was created in response to a Presidential Decision Directive in May 1998 to coordinate the Federal Government's initiatives on critical infrastructure assurance. The CIAO's primary areas of focus are to raise issues that cut across industry sectors and ensure a cohesive approach to achieving continuity in delivering critical infrastructure services. CIAO's major initiatives are to:

- Coordinate and implement the national strategy
- Assess the U.S. Government's own risk exposure and dependencies on critical infrastructure
- Raise awareness and educate public understanding and participation in critical infrastructure protection efforts
- Coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors

CIAO's role was recently expanded with the establishment of The President's Critical Infrastructure Protection Board by Executive Order 13231.

In February 2003, the Board released the "[National Strategy to Secure Cyberspace](#)" to the public.

A part of the CIAO is the Partnership for Critical Infrastructure Security (PCIS)

<http://www.pcis.org/>. The mission of the Partnership is to coordinate cross-sector initiatives and complement public-private efforts to promote the assurance of reliable provisions of critical

infrastructure services in the face of emerging risks to economic and national security. The PCIS played a unique role in facilitating the private sector input to this Strategy.

In September 2006, the PCIS published the [PCIS Governing Principles for Information Sharing](#), for information sharing between and among the critical infrastructure sectors and with government. These governing principles provide a policy level framework for describing the need to share information through secure and effective collection, analysis, and dissemination processes. These governing principles are intended to guide private-sector representatives building or strengthening cross-sector information-sharing capabilities.

Homeland Security Presidential Directive/HSPD-7: On December 17, 2003 the President issued HSPD-7 establishing a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Under this directive, the Homeland Security Secretary is required to coordinate protection activities for each of the following critical infrastructure sectors: information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. The Department and Sector-Specific Agencies must collaborate with the private sector and continue to support sector-coordinating mechanisms to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

<http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html>

#### **6. National Information Assurance Partnership (NIAP)**

<http://niap.nist.gov/>

The National Information Assurance Partnership is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA)

#### **7. National Institute of Standards and Technology (NIST)**

##### **NIST Computer Security Resource Center – (CSRC)**

<http://csrc.nist.gov/fasp>

The Federal Agency Security Practices (FASP) effort was initiated as a result of the success of the Federal CIO Council's Federal Best Security Practices pilot effort to identify, evaluate, and disseminate best practices for security.

##### **NIST Federal Agency Security Best Practices**

##### **800 Series of Special Publications**

<http://csrc.nist.gov/publications/nistpubs/index.html>

SP 800-64, Security Considerations in the Information System Development Life Cycle.

SP 800-51 Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, September 2002

SP 800-50, Building an Information Technology Security Awareness and Training Program

SP 800-47 Security Guide for Interconnecting Information Technology Systems, September 2002

SP 800-46 Security for Telecommuting and Broadband Communications, September 2002  
SP 800-45 Guidelines on Electronic Mail Security, September 2002  
SP 800-44 Guidelines on Securing Public Web Servers, September 2002  
SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002  
SP 800-40 Procedures for Handling Security Patches September 2002  
SP 800-34 Contingency Planning Guide for Information Technology Systems, June 2002  
**DRAFT NIST Computer Security Documents** <http://csrc.ncsl.nist.gov/publications/drafts.html>  
DRAFT SP 800-38B Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode, October 18, 2002  
DRAFT SP 800-36 Guide to Selecting IT Security Products October 9, 2002  
DRAFT SP 800-35 Guide to IT Security Services, October 9, 2002  
DRAFT SP 800-4A Security Considerations in Federal Information Technology Procurements, October 9, 2002  
DRAFT SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, July 24, 2002  
DRAFT SP 800-42 Guideline on Network Security Testing , February 4, 2002  
DRAFT SP 800-43 System Administration Guidance for Windows 2000 Professional, January 28, 2002  
FIRST DRAFT of NIST Special Publication 800-61, Computer Security Incident Handling Guide [IncidentHandlingPub800-61@nist.gov](http://IncidentHandlingPub800-61@nist.gov).  
FIRST DRAFT of [NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems](http://NIST%20Special%20Publication%20800-53,%20Recommended%20Security%20Controls%20for%20Federal%20Information%20Systems).

### **8. National Security Agency (NSA)**

<http://www.nsa.gov>

NSA provides solutions, products and services, and conducts defensive information operations, to achieve Information Assurance for information infrastructures critical to U.S. National Security interests.

#### **NSA Security Recommendation Guides**

NSA maintains a set of recommendation guides for securing a number of computer operating systems, routers, email and executable content.

<http://www.nsa.gov/snac/>

### **9. Centers for Medicare & Medicaid Services:**

<http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>

HIPAA Regulations & Standards: HIPAA Security Rule

The Final Rule adopting HIPAA standards for the security of electronic health information specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.

Other Organizations

### **10. CERT® Coordination Center**

<http://www.cert.org/>

The Computer Emergency Response Team Coordination Center (CERT/CC®) is a center of Internet security expertise, located at the Software Engineering Institute (SEI), a federally funded research and development center operated by Carnegie Mellon University. Its activities include protecting systems against potential problems, reacting to current problems, and predicting future problems. Its work

involves handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing information and training to help improve security. The present CERT Coordination Center grew from a small computer emergency response team formed at the SEI by the Defense Advanced Research Projects Agency (DARPA) in 1988.

#### **CERT® Security Improvement Modules**

<http://www.cert.org/security-improvement/#modules>

#### **The OCTAVE Method of Self-Directed Information Security Risk Evaluation**

<http://www.cert.org/octave/omig.html>

#### **11. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)**

Made available by Carnegie Mellon's CERT Coordination Center ([www.cert.org/octave](http://www.cert.org/octave)), OCTAVE provides measures based on accepted best practices for evaluating security programs.

#### **12. Center for Internet Security (CIS)**

<http://www.cisecurity.org/>

The mission of the Center for Internet Security is to help organizations around the world effectively manage the risks related to information security. CIS provides methods and tools to improve, measure, monitor, and compare the security status of your Internet-connected systems and appliances, plus those of your business partners. CIS is not tied to any proprietary product or service. It manages a consensus process whereby members identify security threats of greatest concern, then participate in development of practical methods to reduce the threats. This consensus process is already in use and has proved viable in creating Internet security benchmarks available for widespread adoption.

CIS Security Benchmarks are technical configuration standards for operating systems, network devices and applications. The Benchmarks are user originated, widely accepted, and reflect the consensus of expert users worldwide. CIS Certified Security Software Products have been independently tested to accurately measure and report the conformity of computer configurations with the technical settings and actions defined in CIS Security Benchmarks.

#### **13. Computer Security Institute (CSI)**

<http://www.gocsi.com/>

CSI is a membership organization specifically dedicated to serving and training the information, computer and network security professional. Since 1974, CSI has been providing education and aggressively advocating the critical importance of protecting information assets. CSI publishes a newsletter, quarterly journal, buyers guide, as well as surveys and reports on topics such as computer crime and an information security program assessment tool.

#### **14. Disaster Recovery Institute – International (DRII)**

<http://www.dr.org/>

DRII was founded in 1988 to provide a base of common knowledge in contingency planning which it makes available via its web site.

#### **15. Information Systems Security Association (ISSA)**

<http://www.issa.org/>

ISSA is a not-for-profit international organization of information security professionals and practitioners. It provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

**16. Information Assurance Technical Framework Forum (IATFF)**

<http://www.iatf.net/>

The Information Assurance Technical Framework Forum is a National Security Agency (NSA) sponsored outreach activity designed to created to foster dialog amongst U.S. Government agencies and U.S. Industry seeking to provide their customers solutions for information assurance problems. The ultimate objective of the IATFF is to agree on a framework for information assurance solutions that meet customer's needs and foster the development and use of solutions that are compatible with the framework.

[http://www.iatf.net/framework\\_docs/version-3\\_1/index.cfm](http://www.iatf.net/framework_docs/version-3_1/index.cfm)

**17. International Information Security Foundation (I<sup>2</sup>SF)**

<http://www.isc2.org/>

I<sup>2</sup>SF sponsored the development of a set of Generally Accepted System Security Principles.

**Generally Accepted System Security Principles**

<http://web.mit.edu/security/www/gassp1.html>

**18. National Cyber Security Alliance**

The National Cyber Security Alliance is a cooperative effort between industry and government organizations to foster awareness of cyber security through educational outreach and public awareness. The Alliance has posted recommendations for securing personal computers - "Stay Safe On-line"

<http://www.staysafeonline.info/>

**19. Open Web Application Security Project (OWASP)**

<http://www.owasp.org/>

The Open Web Application Security Project (OWASP) is an [Open Source](#) community project staffed entirely by volunteers from across the world. The project is developing software tools and knowledge based documentation that helps people secure web applications and web services. Much of the work is driven by discussions on the [Web Application Security](#) list. OWASP has released [Guide to Building Secure Web Applications V 1.1.1](#) in which includes the their list of "Top Ten Web Vulnerabilities".

**20. SANS (SysAdmin, Audit, Network, Security) Institute**

<http://www.sans.org/>

SANS is a research and educational organization. Many of its resources, such as papers, digests, alerts, and studies are available at its web site.

**SANS Model Policies**

<http://www.sans.org/resources/policies/>

**SANS/FBI The Twenty Most Critical Internet Security Vulnerabilities ~ The Experts' Consensus**

<http://www.sans.org/top20>

**Tools to find the top twenty vulnerabilities on your systems and networks.**

<http://www.sans.org/top20/tools.pdf>

**Internet Storm Center**

<http://isc.incidents.org/>

The Internet Storm Center gathers more than 3,000,000 intrusion detection log entries every day. It is rapidly expanding in a quest to do a better job of finding new storms faster, isolating the sites that are used for attacks, and providing authoritative data on the types of attacks that are being mounted against computers in various industries and regions around the globe. Internet Storm Center is a free service to the Internet community. The work is supported by the SANS Institute from tuition paid by students attending SANS security education programs.

**21. Control Objectives for Information and (Related) Technology (COBIT)**

Developed by IT auditors and made available through the Information Systems Audit and Control Association ([www.isaca.org/cobit.htm](http://www.isaca.org/cobit.htm)), COBIT provides a framework for assessing a security program, developing a performance baseline and measuring performance over time.

**22. The Internet Engineering Task Force (IETF)**

is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.).

<http://www.ietf.org/overview.html>

**23. Information Systems Audit and Control Association (ISACA)**

<http://www.isaca.org/>

**24. HIMSS Security Task Force**

Certified in Healthcare Security (CHS)

[http://www.himss.org/asp/certification\\_about.asp](http://www.himss.org/asp/certification_about.asp)

**25. AHIMA Privacy Task Force**

Certified in Healthcare Privacy (CHP)

Certified in Healthcare Privacy & Security (CHPS) – Jointly sponsored by HIMSS & AHIMA

[http://www.himss.org/asp/certification\\_about.asp](http://www.himss.org/asp/certification_about.asp)

**26. Commonly Accepted Security Practices & Recommendations (CASPR)**

<http://www.caspr.org>

The CASPR project is trying to distill information security knowledge into a series of papers available to all (under the GNU FDL license, so that future document derivatives will continue to be available to all). This is a relatively new effort and no documents are yet available.

*27. For the Record Protecting Electronic Health Information*

*Computer Science and Telecommunications Board*

National Research Council

<http://www.nap.edu/catalog/5595.html>

This book was published in 1997. It contains an analysis of the state of healthcare security in place at several leading healthcare organizations. Its chapter six which provides recommendations for current and future healthcare security practices, served as the foundation for the DHHS Proposed HIPAA Security Standard.