

Eight Steps to Integrating Security Standards

Joe Happ

The Health Insurance Reform: Security Standards (45 CFR parts 160, 162 and 164) establishes standards for the security of electronic Protected Health Information (ePHI) to be implemented by health plans, healthcare clearinghouses, and certain healthcare providers.¹ The security standard implements some of the requirements of the Administrative Simplification subtitle in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These security rules became effective April 21, 2003, and compliance was expected by April 21,

2005. Are you compliant? Have you even started your compliance efforts?

Some of us may be assuming these standards only apply to our enterprise clinical data systems; therefore clinical engineering is not affected—that’s IT’s problem. If you are in that category let me share this statement from the security standards: “Covered entities must ensure the confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, or transmits.”¹

With the constant integration of information technologies into traditional biomedical devices, many of them now possess all four of the above attributes. Unless you have passed on all support responsibilities for medical equipment to your IT personnel, you are affected.

In this article, we will discuss the preliminary steps necessary to begin integrating the HIPAA security standards into your clinical engineering program. Getting started on any project of this size and complexity requires commitment throughout the organization to ensure success.

Step 1: Knowledge is King

The security standards are broad in scope, yet very detailed in their compliance requirements. Acquiring a knowledgeable understanding of the security standards will help demystify the task ahead. Several valuable sources of information, implementation strategies, and tools are available to help get you started.²

Step 2: Get Involved

Your IT department has probably already started addressing the enterprise data systems, and will soon (if not already) be approaching you to integrate your information and strategies with theirs. This multi-disciplinary effort should be coordinated in the overall security management program overseen by the institution’s designated security officer.¹ If not already invited, volunteer to become a participating member of this committee.

Equip. Description:		
Manufacturer:		
Model:		
Identify all individually identifiable patient data elements that are stored or transmitted by this device; Circle Yes or No		
Name:	Y	N
Treatment Date:	Y	N
Medical Record #:	Y	N
Patient Account #:	Y	N
Patient Address or Location:	Y	N
Patient Image w/ identifier:	Y	N
If you circled No to All, STOP		
Indicate all storage, transmit, and receive features that exist on this device		
Hard Drive	Y	N
Floppy Diskette	Y	N
Tape	Y	N
Modem	Y	N
Serial Cable	Y	N
PC Card / Memory Stick	Y	N
Wired network (LAN / WAN)	Y	N
Wireless network connection	Y	N
CD ROM / DVD / Optical Drive	Y	N
RAM Memory	Y	N
Print w/identifier	Y	N

Figure 1. Data collection form

Joe Happ, MS, CBET, is clinical engineering director at Health Alliance/Genesis in Cincinnati, OH.

Required Policies Identified

Administrative

Security Management Process Policy
 Assigned Security Responsibility Policy
 Information Access Management Policy
 Security Incident Policy
 Contingency Plan
 Evaluation of Standards Policy
 Business Associate Contracts and
 Other Arrangements Policy

Physical

Facility Access Controls
 Workstation Use Policy
 Device and Media Controls Policy

Technical Safeguards

Access Control Policy
 Integrity Policy

Organizational Requirements

Business Associate Contracts Policy

Documentation

Policy and Procedure Updates/Availability

Figure 2. Checklist of required policies

Step 3: Plan Your Efforts

The fact that these security standards have been mandated as part of our new standard of operation and with resources already strained, carefully integrating this effort into your equipment management program will not only ease the burden but will assure your success. Before commissioning resources, you may want to consider:

- Modifications to your existing inventory database to preserve collected information
- Integrating data collection efforts with other support activities
- Utilizing manufacturers where possible to provide critical data
- Standardizing evaluation methodologies and tools within the organization.

The initial steps must be well planned and implemented for a successful program to emerge.

Step 4: Identify the Bandits

Most medical devices were designed to create electronic patient health information. Their evolution has added capabilities to receive, store, and transmit this information to larger systems for creation of a comprehensive patient health record. Many other devices do not create

ePHI, and may never. Separating your devices in these two major categories will help you divide and conquer.

Our multi-hospital medical equipment inventory consists of approximately 25,000 devices. This inventory represents all devices regardless of whether ePHI is present or not. We initially sorted this inventory by device description, eliminating all types that were easily known not to create ePHI (flow meters, light sources, tourniquets, etc). This first pass created a subset of 7,500 devices that obviously included multiple instances of duplicate models. By performing a query to eliminate duplicates, we were left with 450 unique make and models that required validation.

Step 5: Validate the Data

A preliminary survey needed to be conducted for all 450 make and models to verify if any of the identifiable patient data elements qualifying as ePHI truly existed. Sorting this inventory by manufacturer and model enabled us to hand out manageable portions to our engineers for review.

Using the data collection form shown in Figure 1, our engineers were able to determine which devices actually met the standards criteria. Validation was accomplished by reviewing data provided directly from available manufacturer disclosure statements or from physical verification.³ The resulting inventory of device models served as the core group of items that present a security risk to the institution.

Step 6: Calculating Risk

The security standards require that we: “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity.”¹ An excellent risk scoring methodology utilizing criticality and probability determinants was developed through a collaborative work group of the American College of Clinical Engineering, ECRI, and Health Information and Management Systems Society (HIMSS), and was selected as the basis for our risk assessment effort.^{2,4}

Assessing risk is a relative task that requires knowledge that clinical engineers possess. It also requires a thorough understanding of clinical operations, information system networks, data storage, and operating systems. Utilizing this scoring methodology, a group of our senior engineers applied scores for each device model in the core group of items created in Step 5. Incorporating

Practical Applications

Eight Steps to Integrating Security Standards

the risk scoring results into the equipment database allowed us to permanently attach our results to each device with the same make and model, sort by level of risk, and report our results with a greater range of flexibility.

Step 7: Dust Off Your P&Ps

In order to fully implement the protections mandated in the HIPAA security rules, they must be integrated into the standard operating procedures of our organizations. The policies specifically identified in the body of the final rule are listed in Figure 2. We found many of these were implemented for the enterprise patient information systems, but needed modifications to include the systems and devices found in the medical equipment program.

When procedures became specific to individual systems or devices (access controls, media controls, etc.) it was necessary to develop procedures with the clinical users and append them to the appropriate departmental and administrative policies. This is an ongoing effort.

Step 8: Risk Management Audit

Now that the easy tasks are complete, it's time to roll up your sleeves. The security standards are separated into five categories: administrative, physical, technical, organizational, and documentation. In addition, many of the standards include multiple implementation specifications. Some can be applied universally while others will need to be evaluated individually by system and/or device.

Our validated inventory of stand-alone biomedical devices and clinical information systems sorted by severity of risk provided a natural priority of efforts for this step. Clinical engineers met with equipment users, department managers, and system administrators to review equipment capabilities along with current operational protocols to determine our level of compliance for

			Information Security for Medical Devices & Systems											
Medical Devices & Systems			Phillips Monitoring	Center PACS	Cadwell Sierra Wave	Cartronics CVIS	Watchchild OBIS	GE MUSE	Phillips Tracemaster	Biologic HATS	Biosense Webster EP	BrainLab Vector Vision	Quinton Q-Cath II	
III. Technical Safeguards (164.312)	Access	User ID	98. Systems capable of encryption/decryption?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	
			99. Is encryption/decryption enabled?	Green	Red	Green	Green	Green	Green	Green	Green	Green	Green	Green
	Audit	Controls	100. Systems capable of running audit controls?	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow
			101. Is audit control features enabled?	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow
	Integrity	Authority	102. Mechanisms adopted to ensure against data destruction, RAID1-5, Error correcting mem, Int. diag?	Green	Red	Green	Green	Green	Green	Green	Green	Green	Green	Green
			103. P&P's minimizing risk of EMI damage?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
	Personnel	Authentication	104. Measures to authenticate user via, Token, PIN, Biometrics, Login ID & Password?	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
			105. Mechanism to ensure data is not improperly modified, error correcting Xmit protocols?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Red	Green
			106. Appropriate encryption circumstances defined & identified?	Yellow	Red	Green	Green	Green	Green	Green	Green	Green	Red	Green
			Required	Green	Compliant	Red	Green	Green	Not Compliant	Green	Green	Green	Green	N/A
		Addressable	Green	Compliant	Red	Green	Green	Not Compliant	Green	Green	Green	Green	N/A	

Figure 3. Tool to identify security gaps

each standard. Organizing and analyzing such a large amount of audit data was challenging during this step, therefore we developed a tool that would be useful for identifying security gaps and reporting progress to the organization (Figure 3).

Our next steps will be to make something useful come from all this effort. Our engineers are working collaboratively with manufactures, IT managers, clinical system administrators, and users to determine what security issues exist and what feasible solutions can be implemented. ■

References

1. **U.S. Department of Health and Human Services.** Health Insurance Reform: security standards; final rule. Federal Register, 2003;68(34).
2. **Grimes, S. L.,** HIPAA compliance for biomedical technology: meeting the April 2005 deadline. Overview of the security & risk management process. Paper presented at virtual conference. 2004.
3. **ECRI/ACCE.** Manufacturer disclosure statement for medical device security (MDS2). Available at <http://www.ecri.org/Marketingdocs/MDS2FormInstructions.pdf>. Accessed October 2, 2005.
4. **ECRI/ACCE.** Security Assessment Survey Questionnaire. Available for purchase at: <http://www.ecri.org/>. Accessed October 3, 2005.