# *Keeping Data Secure*
# Protected Health Information And Medical Equipment

Richard Swim

**About the Author**

*Richard Swim, CLES, MCSE, is manager of clinical technology with Baylor Health Care System in, Dallas, TX. E-mail: richards@baylorhealth.edu*

**Maintaining the security of protected health information (PHI) in medical equipment is necessary to maintain a patient's basic right to privacy, and to provide safe, effective care.**

What is the patient's name? What is the patient's age? Is this the right patient record to send vital signs data to? Will the ultrasound images be pulled up for the correct patient when the physician views them? Maintaining the security of protected health information (PHI) in medical equipment is necessary to maintain a patient's basic right to privacy, and to provide safe, effective care. But this very information needed for care of the patient can also lead to adverse consequences if it falls into the hands of those with malicious intent. Names, birth dates, Social Security numbers, and other private information can be used in identity theft, costing the victim dearly in time and money.

PHI may exist in the following list of identifiers, and must be treated with special care.

1. Names
2. All geographical identifiers smaller than a state
3. Dates (other than year) directly related to an individual
4. Phone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers (specific to an individual, such as an implantable device)
14. Web uniform resource locators (URLs) directly related to an individual
15. Internet protocol (IP) address numbers directly related to an individual
16. Biometric identifiers, including finger, retinal, and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

It has always been the responsibility of medical equipment mangers and clinicians to keep PHI confidential in order to protect a patient's right to privacy. There are now regulatory requirements in place that emphasize this responsibility, and they include the possibility of severe penalties for breaches of information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was one of the first regulatory requirements establishing standards for the protection of certain health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act emphasizes government leadership for electronic interchange and security of PHI. As part of the HITECH Act, the Office of the National Coordinator for Health Information Technology (ONC) is responsible for creating a nationwide health information technology infrastructure to improve healthcare quality and care coordination. The Office of Civil Rights (OCR) has responsibility for enforcing the original privacy rule under HIPAA, and the new breach notification requirement under HITECH. If patient information is believed to have been accessed through a breach, the Department of Health and Human Services (HHS) must be made aware of the incident, as well as the individuals affected by the breach. If the breach and misuse of PHI is due to willful conduct, penalties may be up to $50,000 per occurrence, and $1.5 million per year, as well as possible imprisonment.

In order to properly protect patient information, a medical equipment manager must first identify which equipment has the capability of storing PHI. Find a way to indicate in your equipment management system the devices that can store PHI. Focus on these devices to gain more knowledge of what type of PHI and how many records can be stored. Refine your inventory to identify the high-risk devices that need immediate action for increased security of PHI. High-risk devices are those that store multiple records containing PHI, are portable and appealing to the would-be thief. Work with your Office of Information Security (OIS) and corporate compliance teams to form a strategy for moving forward with strengthened security of PHI on these devices.

Many medical devices will have forms of temporary or permanent PHI storage. The devices that retain PHI after a power cycle should be the focus for increased security. PHI storage may be in the form of internal flash memory, internal or external hard drives, or removable USB memory. The smaller a device or its data storage media, the more risk is involved in security of PHI. Many medical devices utilize small notebook computers or components that resemble computers, such as a diagnostic ultrasound. These systems are at high risk of theft due to their portability and similarity to computers. During pre-purchase evaluation, consider the method of data storage a system utilizes and what measures your organization will have to take for security. Request from the vendor the manufacturer disclosure statement for medical device security (MDS2). The MDS2 will make the assessment of the medical device much simpler and help determine security steps. Avoid purchase of systems that require data backups on removable media.

Healthcare technology management professionals have a crucial role to play in keeping patient information secure and confidential within a hospital.

The best method for data storage for a clinical system is client/server architecture. As an example of client/server architecture, consider an endoscopy study system in a procedure area. Data (including PHI) may be stored locally on the computer's hard drive, which will eventually fill to capacity considering the size of endoscopy video studies. Because of the need to free up storage space for new studies, the clinician is challenged with decisions around what to do with those older studies that a physician may desire to review later. External hard drives or USB flash memory storage will be the likely media of choice to resolve the issue. But now the data and PHI is at more risk of loss since it resides on devices that may be misplaced or stolen. A more secure and reliable method of long-term storage is network-mapped hard drives on data center servers. Servers in data centers will be managed through physical/network security and daily backups to ensure your data is available when it is needed. Although there are still considerations for privacy of PHI during use, the worries of long-term storage or loss of PHI will be minimized when the data is not scattered throughout your healthcare system.

**In order to properly protect patient information, a medical equipment manager must first identify which equipment has the capability of storing PHI.**

Not all devices storing PHI will be capable of remote data storage. In those cases, take steps to prevent loss. Physical security is the most basic method. Using a cable that attaches to the device and a desktop or other structure will minimize the possibility of loss of the complete device and its stored PHI.

Beyond physical security, consider additional measures of security. Computer storage should be encrypted, which renders data useless without proper credentials. Some medical device manufacturers will not currently support encryption due to performance issues or system design. Work with these vendors to improve their future system designs to incorporate encryption. At a minimum, computer-based clinical systems should have anti-virus/anti-spyware software installed. This can help prevent Trojans, worms or viruses, and other malware that may track user ID and passwords, and possibly put PHI on the computer at risk. Most manufacturers will define directories for anti-virus scanning exclusion to maximize system performance.

Where possible, use your organization's user credentials for login to keep anonymous users off your enterprise network. In the case of multiple users for a system, such as a patient monitoring central, ensure the system will power up into the monitoring application automatically without access to the underlying operating system. Ensure that service user accounts utilize strong passwords comprised of alphanumerics with a mix of upper/lower-case and special characters.

Once you have taken measures to secure PHI from unintentional loss, don't overlook your own organization's processes for transportation of medical devices with PHI storage.

Once you have taken measures to secure PHI from unintentional loss, don't overlook your own organization's processes for transportation of medical devices with PHI storage. Devices are often returned to vendors for service at their facility. Manufacturers must enter into an agreement with the healthcare organization to keep PHI confidential through a business associate agreement. Having a business partner transport the device for service will meet the need for PHI security, but when a third party is introduced for transport of the device, the security process is broken. If a device containing PHI requires third-party handling, PHI must be protected. If possible, removal and retention of the data storage media is the best method. Otherwise, software destruction of the data is acceptable. The manufacturer may reinstall the operating system and application after device service. Don't overlook demo systems that connect into your organization's clinical network that may collect patient information. Prior to the demonstration enter into an agreement with the vendor that their system's data storage will undergo software destruction prior to removal from your facility.

Be aware of PHI that resides in the medical equipment that you manage. Taking steps to secure this information will take some effort, but is well worth the investment to save time and money in the future, protect patients' privacy, and help provide them the best experience while in your facility. ■

## Resources

For more information on PHI security, visit:

- **HHS** – U.S. Department of Health & Human Services
  www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- **HIMSS** – Healthcare Information and Management Systems Society
  www.himss.org/ASP/topics_FocusDynamic.asp?faid=99
- **IHE** – Integrating the Healthcare Enterprise
  http://IHE.netMedical Equipment Management (MEM): Cyber Security White Paper
- **HITRUST** – Health Information Trust Alliance - http://hitrustalliance.net
- **CE-IT** – Clinical Engineering/Information Technology Collaboration
  http://ceitcollaboration.org
- **FDA** – Cybersecurity Guidance for Networked Medical Devices
  www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070634.htm

***New Edition!***

# BMET Study Guide

## Preparing for Certification And Sharpening Your Skills

The updated and expanded 2012 BMET Study Guide tests your knowledge of five key areas:

- Anatomy & Physiology
- Medical Equipment Function & Operation
- Safety in Healthcare Facilities
- Medical Equipment Problem Solving
- Electronics & Electrical Fundamentals

The CD features 574 interactive questions and answers—each with a detailed explanation—and nearly 200 new and revised questions.

If you manage healthcare technology, or supervise people who do, this educational tool is for you!

**Order code: SGCD**
**List $160 / AAMI member $90**

**To order call +1-877-249-8226 or visit www.aami.org/publications/books/bmetcd.html**

**A Special Thanks to the Sponsors of this CD:**
ARAMARK Healthcare Technologies, CREST Services, and Stephens International Recruiting Inc.

AAMI
Advancing Safety in Medical Technology

AAMI
Advancing Safety in Medical Technology

# Leading Practices

AAMI
Leading Practices
CAPA Verification
Quality Audits
Strategy for Ensuring Effectiveness and Compliance of Quality System

*AAMI's Leading Practices series provides practical and concise peer-reviewed information on specific topics important to HTM professionals. Designed to give quick, easy-to-follow pointers, these documents also include graphics, charts, and forms that illustrate each topic.*

## CAPA Verification and Validation: Practical Approaches to Compliance

Designed to help medical device firms better understand, implement, and comply with the Corrective and Preventive Action (CAPA) section of the Quality System Regulation (21 CFR 820.100).

**Order Code: LP-CAPA or LP-CAPA-PDF**
**List $70 / AAMI member $35**

## Management Responsibility: Connecting Business Acuity and Quality Excellence

Designed to highlight for medical device firms the role of top management in ensuring effective and compliant operation of the Quality Management System.

**Order Code: LP-MR or LP-MR-PDF**
**List $70 / AAMI member $35**

## Quality Audits: Strategy for Ensuring Effectiveness and Compliance of Quality System

Discusses the need for manufacturers to conduct regular quality audits led by individuals not directly responsible for the matters being audited, with management review of audit results.

**Order Code: LP-QA or LP-QA-PDF**
**List $70 / AAMI member $35**

## Practical Approaches to Compliance: CAPA—Complaints

Reviews the four most frequently cited observations related to Complaint Files, and provides examples and helpful tools for an effective complaint handling system.

**Order Code: LP-COMPLAINT or LP-COMPLAINT-PDF**
**List $70 / AAMI member $35**

## Order Your Copy Today!

Call +1-877-249-8226 or visit www.aami.org/publications/leadingpractices