Health Information Compliance Alert

Enforcement News: Step-By-Step Guidance Helps You To Make Mobile Devices More Secure

Plus: FDA warns of infusion system at risk for cybersecurity issues.

You'll soon have some new resources at your fingertips to help you make the most of new mobile technologies while staying HIPAA compliant.

On July 23, the **National Cybersecurity Center of Excellence** (NCCoE) released a draft step-by-step guide that's the first in a new series of publications aimed to help healthcare providers make mobile devices more secure. The NCCoE, which was created by the **National Institute of Standards and Technology** (NIST) in 2012, released the draft of "Securing Electronic Health Records on Mobile Devices" for public comment. The comment period ends on Sept. 25.

The series of guides will provide practical advice on how to improve cybersecurity using standards-based, commercially available, or open-source tools, and the first draft guide will focus on how healthcare providers can balance protecting patient information with taking advantage of new communications technologies.

"The NCCoE was established specifically to help organizations solve real-world challenges, and this was one of particular concern to the healthcare community," NCCoE Director **Donna Dodson** said in a July 23 statement. "This guide can help providers protect critical patient information without getting in the way of delivering quality care."

Link: To view the draft guide, go to https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices .

Watch Out For Infusion System's Cybersecurity Vulnerabilities

If your patients use **Hospira**'s Symbiq Infusion System, they could be at risk for a potentially deadly cybersecurity breach.

On July 31, the **U.S. Food and Drug Administration** (FDA) issued an alert warning of potential cybersecurity vulnerabilities regarding the Symbiq Infusion System, a computerized pump for continuous delivery of general infusion therapy to patients and primarily used in hospitals or other acute and non-acute healthcare facilities, including nursing homes and outpatient care centers.

An independent researcher assisted Hospira in confirming that users could access the infusion system remotely through a hospital's network, potentially allowing an unauthorized user to control the device and change dosage levels, according to an Aug. 6 blog posting by attorney **Steven Richard** for the law firm **Nixon Peabody LLP**. Although no known adverse events or unauthorized access of a Symbiq Infusion System have occurred, the potential for a cybersecurity breach could lead to over- or under-infusion of critical patient therapies.

Hospira has discontinued the system's manufacture and distribution for unrelated reasons, and now the FDA is encouraging facilities to begin transitioning to alternative infusion systems, Richard said. During the transition to an alternative infusion system, you should reduce the risk of unauthorized system access by:

- Disconnecting the affected product from the network;
- Ensuring that all unused ports are closed; and

- Monitoring and logging all network traffic attempting to reach the affected products.

Resource: For more information on the FDA's alert regarding the Symbiq Infusion System, go to www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm456832.htm .

New Guide: Get A Handle On HIPAA Basics

Would you like an easy-to-understand summary of the HIPAA Privacy and Security Rules and the Breach Notification Rules? You've got it.

The **HHS Office for Civil Rights** (OCR) recently released a new guide entitled, "HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules."

The new guide "is a nice summary of how HIPAA applies and what is necessary for compliance at a basic level," says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems LLC** in Charlotte, VT. The guide also includes lots of very useful links to other resources and guidance.

"If you're just getting started in HIPAA, this is a good way to get a basic understanding of HIPAA, and then look at the linked guidance for more," Sheldon-Dean notes. You can access the new guide at www.hhs.gov/ocr/privacy/hipaa/understanding/training/hippaprivacysecurity.pdf .

Pay Attention: Unauthorized Access/Disclosures Top Largest Breaches In August

Hold onto your patients' protected health information (PHI) □ the **HHS Office for Civil Rights** (OCR) is tracking the latest large-scale breaches affecting 500 or more individuals. And the results for the month of August signal no slowdown whatsoever in big HIPAA breaches.

Of the 15 large-scale breaches reported to OCR in August, two involved health plans and the remaining 13 affected healthcare providers. Seven breaches involved unauthorized access/disclosure, five involved theft, two involved loss, and one involved a hacking/IT incident.

The largest breach involved the theft of a laptop and affected 160,000 individuals, reported by **Empi Inc and DJO, LLC** in Minnesota, followed by a hacking/IT incident involving a network server that affected 10,000 individuals reported by **Pediatric Group LLC** in Illinois. A computer theft caused a breach of 9,000 individuals' PHI in California, while another 8,345 individuals were affected by a **Walgreen Co.** breach due to unauthorized access/disclosure involving paper/films.

Link: You can view the OCR's Wall of Shame at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf .

Is Password Protection Enough To Prevent HIPAA Breach?

If your laptop is stolen, will simple password protection prevent the thief from accessing or using the protected health information (PHI) stored on the device? Possibly not □ but a recent breach case could inform healthcare providers on how password protection might reduce the consequences of this type of breach.

On Sept. 1, **UCLA Health** announced that it's notifying 1,242 affected patients of the theft of an employee's laptop containing patient names, medical record numbers, and health information used to prepare treatment plans. The laptop, which was password protected, was stolen on July 3.

This breach comes on the heels of a much larger incident that UCLA announced in July, which involved a cyberattack that affected nearly 4.5 million individuals' PHI. UCLA faces a class-action lawsuit as a result of that breach (see "Smarten Up Your Data Retention Policy □ Pronto," HIC Vol. 15, No. 8).

UCLA Health analyzed a backup disk that the employee provided to determine whether PHI or other restricted information was stored on the device. "At this time, there is no evidence that any individual's personal or medical information stored on the laptop has been accessed, disclosed, or used," UCLA's announcement stated. The laptop did not contain any Social Security numbers, health plan ID numbers, credit card numbers, or other financial data.

In addition to notifying affected patients, UCLA also notified the **HHS Office for Civil Rights** (OCR) and the California Attorney General, and set up a dedicated phone line to provide information and assistance to affected individuals who received notification letters. UCLA says it is "enhancing its security policies and retraining those involved with the incident to help avoid any future similar events."