ISSUE
05
SPRING
2015

THE NORTHWEST'S HIPAA SECURITY BULLETIN

HIPAA SAFE

contents

OCR Breach Portal

The Office of Civil Rights (OCR) has updated its website's breach notification portal, the online reporting tool CEs must employ in the event of an unsecured ePHI breach. CEs must report all breaches as detailed in CFR-45 §164.408.

The new portal is significantly different from the previous web page. The website now requests information based on what the CE reports. The breach end date and discovery end date are now required to submit a report. The portal also replaces the previous technology-oriented options with greater focus on what Privacy and Security Rule safeguards were in place at the time of the breach. Finally, more precise response actions are listed than were previously required.

In Summary

Presumably, OCR has developed a tool that will help guide their decision to investigate a breach (or not) and provide an affected CE some insight to OCR's expectations prior to and following an ePHI data breach.

Medical Devices: Overlooked ePHI Assets

Two trends we consistently see in our travels involve an incomplete grasp of two key areas; **electronic protected health information (ePHI) assets** and **how and where medical information is communicated**. Medical devices are often in the middle of this ePHI portfolio oversight. Almost all medical devices either store patient information or transmit to the primary electronic health record system; some appliances forward ePHI to patient management or external billing systems.

When assessing the risk associated with medical devices, we recommend **understanding the device's medical use**, the **environmental and technical controls** that make the device vulnerable, and **how these vulnerabilities affect risk** to ePHI. Many medical device manufacturers are only recently implementing security controls. As a result, most legacy systems cannot be made secure at a reasonable cost and we anticipate that a replacement strategy will become more commonplace for those Covered Entities (CE) desiring to better protect patient data.

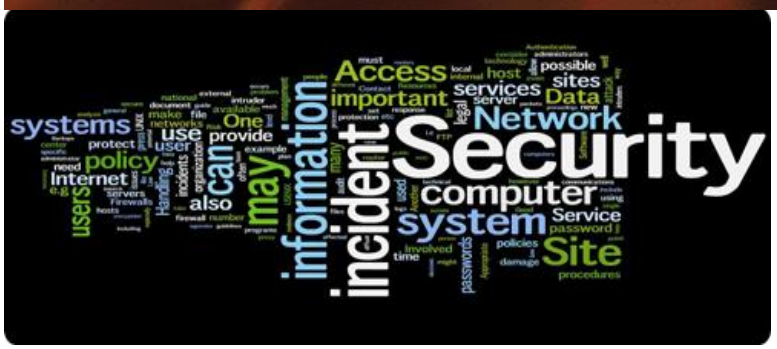
CEs need to **understand at least the following features when evaluating their medical device inventory**:

- Where is the patient data stored?
- Which encryption method(s) is used to store or transmit the ePHI?
- What kind of activity logs are produced and how are they audited?
- What kind of authentication (e.g. credentials) is required to use the system?
- What controls protect an active session?

Once risk from each medical device is documented, **place controls to protect as "reasonable and appropriate"** the affected ePHI.

Medical devices are an integral part of many medical services and need to be considered when planning and executing an information risk management strategy. CEs should **identify all systems that store or transmit ePHI** during the planning phase of their next security risk analysis and **make plans to replace those devices that lack reasonable security controls**.

PROTEUS
CONSULTING
www.ProteusID.com



Security Incident Planning

This quarter's theme of preparing for a patient data breach would not be complete without including the actions that need to be taken to determine whether a breach has occurred.

The Administrative section of the Security Rule includes one standard and one required implementation specification. This means that **security incident management applies to all CEs and BAs.** To be compliant with HIPAA, both need to have policies and procedures to manage security incidents.

Managing incidents does not mean trying to guess all of the potential incident types. We believe it is best to create a repeatable process that includes: how incidents are reported, to whom incidents are reported, what controls (or constraints) will affect the investigation, what internal reports must be completed, and when external support should be requested.

Once an incident response plan is drafted, we recommend ensuring that all details are shared across the organization. After the plan is tentatively approved, it should be tested for effectiveness. This check will most likely uncover new considerations and provide others the opportunity to communicate whether the plan will work (or fail) in their area of expertise. A good incident response plan will integrate communications, legal, and human resources employees. Together, they should advise how evidence will be preserved and used, and how the incident details will be shared internally and externally.

The Security Incident Plan exists to respond to and mitigate actions harmful to the protection of ePHI. All investigations and their outcomes should be maintained and reviewed with the HIPAA Security Officer. Lessons learned should be shared with staff and incorporated into periodic training materials, as recommended by counsel.

2014's 164 ePHI Data Breaches Summarized*

Incidents at a Glance (Credit: Redspin)

◦ **Approximately 9 million patients affected** ◦ **Breaches increased ~25% from 2013**

	No. of Breaches	% of Total	No. of Records	% of Total
Theft	67	40.8%	847,918	9.5%
Unauthorized Access	33	20.1%	2,732,738	30.7%
Hacking or IT Incident	23	14.0%	4,750,716	53.4%
Other	17	10.4%	322,565	3.6%
Loss	16	9.8%	159,124	1.8%
Improper Disposal	8	4.9%	86,549	1.0%
Totals:	164	100%	8,899,610	100%

*Does not include the Anthem breach, where 10 years' worth of customer information was stolen, because no ePHI is yet reported compromised.

Breach Planning

Our newsletter normally focuses exclusively on issues related to the HIPAA Security Rule. Equally important to security is having the tools in place to report a breach, before the event occurs.

The Breach Notification Rule lists four standards and nine implementation specifications that CEs and their Business Associates (BA) must follow in the event of an unsecured ePHI compromise. There are exceptions* to reporting a breach and they include:

- unintentional acquisition by an authorized member, in good faith;
- when retention is not reasonable;
- inadvertent disclosure by and to a person who is authorized to access PHI.

Also worth noting is that this rule applies to information "…that that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance…".

Each CE and their BAs needs to have policy, procedures and training to comply with the HIPAA Breach Notification Rule.

** Please refer to §164.402 for full definitions, which have been shortened to fit into this article.*

Articles by Alan Davis
Proteus Consulting
Hayden, ID 83835
(208) 215.5607