ISSUE
15
AUTUMN
2017

THE
NORTHWEST'S
HIPAA SECURITY
BULLETIN

HIPAA SAFE

CONTENTS

Risk Analysis Pitfalls

We wrote about how to perform a risk analysis (i.e. a risk assessment) in Issue 14. The 2016 Office of Civil Rights (OCR) Audit Protocol clarifies the Security Rule citation and confirms an expectation for:

● a defined scope

● details of identified threats and vulnerabilities

● an impact and likelihood analysis, and

● a risk rating.

The following examples may help improve security and validate a HIPAA Security program, but lack the measures to be considered a bona-fide risk analysis:

● a HIPAA Security Rule compliance evaluation using the 2016 OCR Audit Protocol

● an assessment of information services or technology security controls, even when mapped from a reputable security controls source (e.g. NIST, SANS, etc.) to the Security Rule. This type for work does support §164.308(a)(8), "Evaluation"

● completing a checklist. Risk is not "checked", but calculated.

There are plenty of very thorough information security companies, but we recommend that Covered Entities (CE) and Business Associates (BA) seek a HIPAA dedicated company to help with at least one risk analysis. Understanding what a risk analysis is and is not helps verify a compliant risk analysis project.

Federal Trade Commission's Start with Security

Although technology may update how we protect our systems, good security principles doesn't change with time. We are reminded of this fact while reviewing the Federal Trade Commission's (FTC) 2015 *Start with Security* whitepaper, which provides 10 lessons learned from resolved security cases. We present a summary of this excellent commentary, mapped to applicable HIPAA citations for clarity and relevancy, and recommend a more in-depth read of the source material.

● Start with security: 164.316(a)

● Control access to data sensibly: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B) & (C)

● Require secure passwords and authentication: 164.308(a)(5)(ii)(D)

● Store sensitive personal information securely and protect it during transmission: 164.312(a)(2)(iv), 164.312(e)(2)(ii)

● Segment your network and monitor who's trying to get in and out 164.308(a)(1)(ii)(D)

● Secure remote access to your network 164.312(e)(1)

● Apply sound security practices when developing new products: 164.308(a)(1)(i), 164.308(a)(8)

● Make sure your service providers implement reasonable security measures: 164.308(b)(1), 164.314(a)(1)

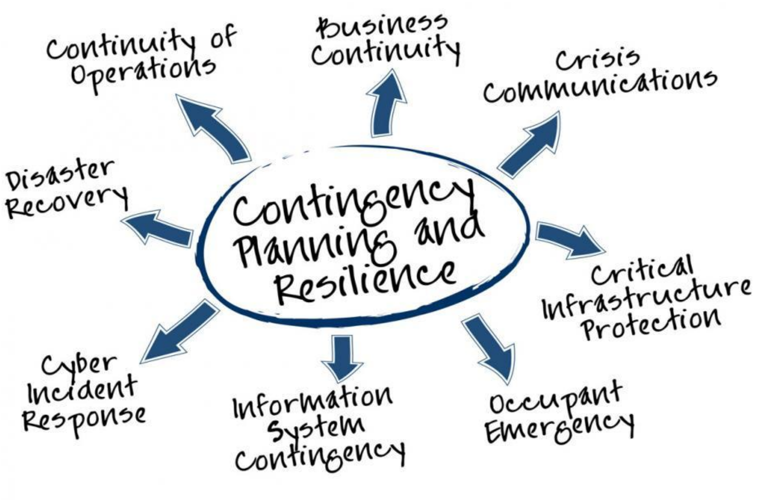
● Put procedures in place to keep your security current and address vulnerabilities that may arise: 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)

● Secure paper, physical media and devices: 164.310(a)(1), 164.310(a)(2)(ii), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii).

A resource external to HIPAA may help security officers communicate the importance of traditional security controls to their organization's leadership and provide a different perspective to the challenges that come with securing electronic protected health information (ePHI).

Although the FTC does not directly enforce HIPAA, they have prosecuted a handful of recent healthcare cases where consumer protections were violated. Their whitepaper is full of lasting concepts and approaches to help protect ePHI.

PROTEUS
CONSULTING
www.ProteusID.com



Criticality Analysis Process

The National Institute of Standards and Technology (NIST) has release a draft model to help organizations prioritize systems and components. As detailed in addressable Security Rule citation 164.308(a)(7)(ii)(E), CE and BA are to assess the relative criticality of applications and data in support of their contingency plan. We see many CE put this important work in the hands of their information services (IS) team or contracted technology support BA, who may not fully understand the business objectives of all ePHI systems. Realizing each system's purpose improves purchase details, risk management, lifecycle decisions and business continuity decisions.

The model consists of five processes (paraphrased):

● **Criticality Analysis Procedure Definition**: develop or adopt a set of procedures to perform criticality analyses

● **Program-Level Criticality Analysis**: define, review and analyze the program to identify key activities vital to reaching its objectives

● **Conduct System-Level Criticality Analysis**: review and analyze the system's criticality relative to the organizational goals

● **Conduct Component-Level Criticality Analysis**: review and analyze system components for their specific system criticality

● **Conduct Detailed Review of Criticality**: create final criticality levels for systems and their components.

This process is not as hard as it sounds, and should involve clinical stakeholders and IS staff to shape important risk management decisions that include but are not limited to recovery point objectives and recovery time objectives. The criticality analysis is a vital part of a healthy HIPAA Security program.

Public comments ended 8.18.17 and our healthcare partners should benefit from another sound NIST reference.

(ePHI) System Audits to Consider

Daily

● Anti-malware deployment

Weekly

● Failed administrator level logins

Monthly

● Active Directory (AD) & EHR failed logins

● Workstation and server security patch deployment

Quarterly

● Workstation physical controls

● Backup media integrity

● System required AD accounts

● Primary EHR accounts

● ePHI access (i.e. ePHI use audit)

● Patient count for each ePHI system

Semiannually

● Tertiary ePHI system accounts

● All non-workforce member accounts

Annually

● Disaster recovery plan & data center access

● Technical and non-technical testing

● Validate security groups' access

These periodicities are only suggestions and your audit cycles should be based on your resources, and on reasonable and appropriate policy and procedures.

Beware the Darknet

We recently attended an interesting presentation given by Stephen Health, a respected information services security leader. Stephen explained what a dark net (also referred to as a dark web) is, how private websites exist outside of normal domain naming systems, how people access these websites, and provided sample websites' content.

The Darknet is not a separate network, but uses the Internet to connect people to each other or to websites using non-standard network ports and protocols. A common program used to communicate a dark web is The Onion Router, more known as Tor.

We don't normally associate HIPAA or hospital networks with dark webs, but we did realize another need for:

● white-listing applications to ensure that Tor friendly clients cannot execute on network endpoints

● controlling which personally owned devices can access the corporate network

● configuring workstations to not run or install unauthorized software

● considering how USB ports are employed and white-listing workstation hardware devices

● disabling all non-essential ports and protocols from the network, and

● training the workforce to understand the dangers involved with non-traditional web browsing.

ARTICLES BY ALAN DAVIS
PROTEUS CONSULTING
HAYDEN, ID 83835
(208) 215.5607