ISSUE
20
WINTER
2018

THE NORTHWEST'S HIPAA SECURITY BULLETIN

HIPAA SAFE

CONTENTS

Business Associate Safeguards

One question that we are routinely asked by our Covered Entity (CE) partner-clients is, "What can we do to reduce the risk that one of our Business Associates (BA) will cause a breach of our electronic protected health information (ePHI)?"

Our response is that all CE should obtain satisfactory assurances that the BA complies with their contracted HIPAA requirements. Assurances begin ahead of contract signature:

- query the Health and Human Services Office of Inspector General's List of Excluded Individual and Entities, and Corporate Integrity Agreement Enforcement websites
- ensure the BA has insurance that covers a data breach event
- ask the BA for references from other CE customers.

We also recommend an annual attestation letter from the BA to CE that includes at least:

- HIPAA Privacy & Security Officer contact information
- when the last risk analysis was completed, if ePHI is involved
- the date of most current HIPAA policy and procedures review, and
- identifying all people by name who need system access, if ePHI is involved.

BA account for more than 20 percent of all breaches and due diligence is a mature HIPAA Security program element.

Compliance, Cyber Security Framework, & Risk

Earlier this year the health insurance company Anthem settled their 2015-reported data breach with Health and Human Services (HHS) for a record $16 million dollars. Equally shocking is the fact that the Anthem breach had begun in 2014, just months after being celebrated as becoming HITRUST certified. HITRUST is an **expensive** healthcare compliance certification that tried unsuccessfully to establish itself as the sole standard to measure HIPAA Security compliance. Luckily, HHS continues to not endorse any specific credentials or compliance framework, although the federal government still authors the NIST approach used by our company. **Demonstrable Security Rule compliance to HHS is the standard to measure a program, but it's not the only consideration for a CE and their ePHI**.

Regardless of their organization's size, a HIPAA security officer should be aware of the cybersecurity framework (CSF) elements employed to protect patient information. There are a handful of CSF (SANS, NIST, COBIT, etc.) and even a small organization can adopt the SANS CIS Critical Controls for Effective Cyber Defense. We realize that most HIPAA or compliance officers aren't necessarily CSF experts and that many may rely on in-house information technology teams or contracted technology service providers, but our point is that **a mature HIPAA security program includes actionable and routine traditional information security work based on a CSF**.

The Security Rule's required Risk Analysis citation aside, **both compliance and security need to be viewed from the perspective of risk**; specifically, the risk of unauthorized disclosure, of harm to a CE or BA reputation, of lost revenue and myriad other legal issues. But **risk has to be managed** by: accepting, transferring, avoiding or mitigating. Each term has specific technical meaning that needs to be well understood before considering.

It is our experience that many CE will better realize the Security Rule's real value to healthcare by viewing their program from all three of these perspectives.

PROTEUS
CONSULTING
www.ProteusID.com

HHS Releases HICP

December 28th marked the HHS release of their four volume Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication. This new technical collection is meant to provide voluntary cybersecurity practices for all healthcare entities ranging from a small clinic to hospital systems and was borne from a two-year public and private sector collaboration aimed at cost effectively reducing risk to ePHI.

Janet Vogal, HHS' Acting Chief Information Security Officer reports, "Cybersecurity is everyone's responsibility. It is the responsibility of every organization working in healthcare and public health. In all of our efforts, we must recognize and leverage the value of partnerships among government and industry stakeholders to tackle the shared problems collaboratively."

Technology has simultaneously the power to advance lifesaving practices and to be a new foothold for criminals to exploit; as such, HIPAA needs to be more than a compliance program or a means to government funding reimbursement.

The HICP's main volume discusses the top five current threats and recommends 10 practices to manage these threats. It uses statistics to show how unauthorized disclosure affects finances and patient care.

Two technical volumes are aimed at the information services / technology security workforce; one provides guidance to smaller healthcare entities and the second to medium and large organizations.

The fourth HICP volume showcases resources and templates that all healthcare companies can utilize to assess their CSF maturity.

Please visit the HHS website (hhs.gov) to learn more.

After a Very Quiet Year, OCR Settlements Surge in Q4

Pagosa Springs Medical Center
- Didn't terminate ePHI access / no BA contract
- 557 patients compromised
- Paid $111.4K and entered into 2 year CAP

Advanced Care Hospitalists
- No BA contract or BA policy
- Up to 9,255 patients compromised
- Paid $500K and entered into 2 year CAP

Allergy Associates of Hartford
- Physician commented to press
- One patient compromised
- Paid $125K and entered into 2 year CAP

Anthem, Inc.
- Failure to manage security incidents
- Cyberattacks compromised 79M patients
- Paid $16M and entered into 2 year CAP

Three Separate Northeast Hospitals
- Lack of patient consent to be filmed for television show
- Paid $999K (divided) and each has a CAP

"After watching 2018 activity, we cannot predict how regularly OCR will settle future breach cases. We can however continue to advocate a strong HIPAA Security program in 2019."

HIPAA as a Standard of (ePHI) Care

One of the consequences from most ePHI breaches is the civil lawsuit(s) brought against the company responsible for protecting the information. However, there is no HIPAA Rules' citation that directly allows citizens to sue for damages resulting from a breach of PHI or ePHI. But various courts have recognized HIPAA as a "standard of care" or set of reasonable controls and used these standards to litigate data breach cases.

The first multistate suit was initiated in 2018 by attorneys general (AG) in 12 states, alleging that Indiana company Medical Informatics Engineering and its subsidiary NoMoreClipBoard failed to protect 3.9 million patients' ePHI through its WebChart web application. In addition to potentially using HIPAA as a standard of care, the AG are citing state laws including: notice of breach statues, personal information protection acts and unfair and deceptive practice laws.

Failing to protect PHI and ePHI can lead to more trouble than from HHS and as this example demonstrates, many state AG are compensating for the lack of a more aggressive or proactive HHS breach enforcement program.

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