ISSUE
18
SUMMER
2018

THE NORTHWEST'S HIPAA SECURITY BULLETIN

HIPAA SAFE

CONTENTS

Philips Vulnerabilities

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ISC-CERT) issued security advisories at the end of March (ICSMA-18-088-01 and ICSMA-18-086-01), advising that Philips has discovered vulnerabilities in its iSite and IntelliSpace PACS medical imaging archiving systems and its Alice 6 polysomnography system.

Criminals can inject software instructions that affect iSite and IntelliSpace PACS system control flow and exploit flaws that could compromised electronic protected health information (ePHI) or the system's availability. Philips acknowledged the Alice 6 system lacked proper the authentication and data encryption required to protect the stored user credentials and personal information.

To resolve the issues related with the iSite and IntelliSpace PACS systems, Philips has advised that its customers ensure that all software patches are current on any affected system(s) and to upgrade to the IntelliSpace PACS 4.4.55x with Windows 2012. Philips also advised customers with the Alice 6 system to implement network security practices and limit network access, and that the company plans to release a new system version to mitigate vulnerabilities by the end of the calendar year.

HIPAA Privacy and Substance Use Disorder Information

The HIPAA Rules that govern Covered Entities (CE) and Business Associates (BA) are found in the Code of Federal Regulations (CFR), Title 45, Public Welfare. But CFR Title 42, Public Health, places additional restrictions upon the disclosure and use of substance use disorder (SUD) patient records which are maintained in connection with the performance of any part 2 program. **As data sharing continues to evolve in the medical community, HIPAA security officers whose organizations work with SUD organizations need to understand this additional regulation**.

Additionally, last May the House Energy and Commerce Committee's health subcommittee hosted comments supporting the Overdose Prevention and Patient Safety Act (HR 3545), which seeks to amend the 42 CFR Part 2 and better align it with HIPAA. Legislation proponents have raised concerns that a SUD treatment patient's healthcare is negatively affected because the treating physician cannot see an entire medical history and treatment. HR3545 seeks to "treat SUD medical records that relate to treatment, payment or healthcare operations in the exact manner as all other medical records", according to Oregon Representative Earl Blumenaur. HR3545 will also strengthen Part 2 unauthorized disclosure penalties. Opponents fear changing Part 2 privacy will discourage patients from seeking SUD treatment or could increase the risk that leaked SUD information could negatively affect employment, housing, child custody and risk other forms of discrimination.

Whether SUD treatment patient information remains separated from traditional physical health records remains to be seen. The bill, which was introduced in July of 2017, is still being considered by the health subcommittee. **Worth noting is the often close relationship between mental health and SUD treatment facilities and organizations**.

https://www.govtrack.us/congress/bills/115/hr3545 provides more information and legislation status.

PROTEUS CONSULTING
www.ProteusID.com

Potential HIPAA Rule Changes

Roger Servino, the Office of Civil Rights (OCR) Director, recently briefed three policy proposals being considered:

- how OCR might distribute a percentage of the funds it collects from settlements and civil monetary penalties to patients affected by breaches
- changing or dropping the current "notices of privacy practices" (NPP) HIPAA Privacy Rule requirement
- clarifying when "good faith" PHI disclosures are permitted without patient consent.

The HITECH Act opened the door for OCR to supplement enforcement actions with monies collected through settlements and civil monetary penalties. These funds can also be used to compensate breach victims, but some are concerned that the potentially small amount of available dollars per person will worsen a breach event.

The benefit provided by the notices of privacy practices is being questioned. Servino has received feedback that the requirement often causes confusion among patients that read the form, or that patients sign the form without understanding its contents. Patients and physicians want processes that better patient health, so the NPP may not remain an OCR requirement.

The opioid abuse frequency is one catalyst of the desire to improve guidance to CEs that are hesitant to share PHI for crisis treatment cases. Families are often unaware when a person has repeated drug overdoses and many people believe that patient outcomes can be improved when the patient can benefit from an informed support team helping with treatment and recovery. We hope that common and reasonable examples are included to aid physicians' decision making.

The OCR is seeking public and healthcare industry comments before advancing the three policy initiatives. While not directly a HIPAA security issues, these ideas if enacted would become significant news to share with all healthcare providers.

University of Texas MD Anderson Cancer Center Case

Breach(es) Details

- Two unencrypted thumb drives missing
- One unaccounted for unencrypted laptop
- 35,000 patients affected
- An encryption policy existed for six years prior

$4.3M Civil Monetary Penalty

- $2,000 for each day from March 24th, 2011 through January 25th, 2013
- $1.5M for years 2012 and 2013 – the maximum allowed by law
- Judge called slow policy implementation "shocking"

How Proteus Consulting Can Help

- Policy and procedure creation or review
- Risk identification through a risk analysis
- Risk register review with reasonable and appropriate response actions to reduce ePHI unauthorized disclosure (breach) risk
- Project management processes supporting risk register solution(s) implementation

"Policy and procedures must be followed up with training and accountable processes to reduce unauthorized disclosure risk." – Proteus Consulting

Washington State Law SB 6027

June 7th saw the enactment of a new Washington State law to protect medical and mental health information to strengthen patient privacy rights.

The main reason cited for this legislation was related to civil suits. Corporate attorneys, while defending their clients, would often investigate a plaintiff's past to advance their client's defense. In some cases, plaintiff private therapy session information was entered into court records. This "discovery" defense tactic and the information released was especially effective to persuade a plaintiff with a potentially legitimate claim, especially in the case of a sexual harassment complaint, to withdraw their charges.

Defense attorneys remain concerned that introducing medical information was helpful to challenging cause and magnitude of alleged damages. They also assert that a judge has the ability to determine whether the information is relevant to the case.

The new law does allow for information less than two years old under three specific plaintiff claims:

- a specific and diagnosable physical or psychiatric injury related to the defendant's conduct
- a need to rely on provider or expert witness record or testimony to seek damages, or
- alleged failure to accommodate a disability or discrimination for same.

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