NOVEMBER
2021

MIDLAND HEALTH
Compliance Hotline
877•780•9367

COMPLIANCE CONNECTION

This newsletter is prepared by the Midland Health Compliance Department and is intended to provide relevant HIPAA privacy issues and hot topics.

IN THIS ISSUE

HIPAA Privacy Rule
Myths & Facts

Myth

"The Notice of Privacy Practices does not need to be posted in the provider's facility or on the website if it's otherwise available."

Fact

Not true!
HIPAA is clear about this.
The NPP must be posted in the facility
and in a prominent place
on a provider's website,
in addition to being provided
in writing to patients.

Resource:
https://thehipaatool.com/beware-hipaa-myths/

NOVEMBER 7–13, 2021
CORPORATE COMPLIANCE & ETHICS WEEK
Awareness, Recognition, Reinforcement

Corporate Compliance & Ethics Week
November 7–13, 2021

CORPORATE COMPLIANCE AND ETHICS WEEK—WHAT'S IT ALL ABOUT?

A short history: The "official" Corporate Compliance and Ethics Week was first observed in 2005 as an event that could assist members of HCCA and SCCE with the need to educate staff on the importance of compliance and ethics. But the event's roots actually go back to 2002, when two HCCA members, Gene DeLaddy and Cheryl Atkinson, wrote an article for Compliance Today telling others about an awareness program at their facility. That event was called Compliance Awareness Week, and it was celebrated at the Carolinas HealthCare System in Charlotte, North Carolina.

The first National Corporate Compliance and Ethics Week was launched May 22-28, 2005. HCCA and SCCE have always co-sponsored the event, and early-on, took steps to sponsor a resolution in the U.S. Senate. That resolution would have allowed a National Corporate Compliance and Ethics week to be officially recognized by Congress. Unfortunately, the senators who were shepherding the proposed resolution left office before it made its way through. But by that time, Corporate Compliance and Ethics Week had taken hold among members of both HCCA and SCCE, and compliance professionals across the country. In the early years, the event was celebrated during the last full week of May. It was later moved to the first full week of May to avoid Memorial Day.

Why celebrate? Corporate Compliance and Ethics Week offers a great opportunity to shine a spotlight on the importance of compliance and ethics at organizations. By having a designated week, the compliance staff can build awareness in ways that reinforce not just specific rules and regulations, but an overall culture of compliance. Using the "hook" of ***"Corporate Compliance and Ethics Week,"*** emphasizes the overall message in several different ways. The importance of employee education is emphasized by the U.S. Federal Sentencing Guidelines' seven elements of an effective compliance and ethics program. The education element requires that steps be taken so all employees know and understand the compliance and ethics standards that they are expected to meet. With a week-long celebration of compliance and ethics, provides a great opportunity to introduce and reinforce chosen themes and basic goals including:

- ***Awareness*** – of the Code of Conduct, relevant laws/regulations, hotlines and other reporting methods, the organization's compliance and ethics staff, etc.
- ***Recognition*** – of training completion, compliance and ethics successes, etc.
- ***Reinforcement*** – of the culture of compliance for which the organization strives.

Resource:
https://assets.hcca-info.org/portals/0/pdfs/resources/ccew/whycelebrate.pdf

DID YOU KNOW…

HIPAA Enforcement Is Up 400 Percent

As we continue modernizing healthcare infrastructure and moving a growing list of systems into the digital space, healthcare operators continue to open themselves up to vulnerabilities. As a result, HIPAA enforcement is stronger than ever before, and the Department of Health and Human Services has made enforcement of these regulations a priority.

Resource: https://www.cloudnexusit.com/2020/12/31/hipaa-fun-facts/

MIDLAND
HEALTH

NEWS

Stolen Laptop Contained the PHI of Dignity Health Patients

Resource Anesthesiology Associates (RAA) of California has started notifying certain patients of Dignity Health's Mercy Hospital Downtown and Mercy Hospital Southwest that some of their protected health information was stored on a laptop computer that was stolen.

RAA of California provides anesthesiology services at the Dignity Health hospitals, which requires access to patient data. On July 8, the laptop was stolen from an RAA of California administrator. The theft was reported to law enforcement, but the device has not been recovered.

RAA of California conducted an investigation to determine which patient information was stored on the device and could potentially be accessed. The review confirmed the following types of information were stored on the device: Names, addresses, dates of birth, provider names, dates of service, diagnoses and treatment information, health insurance information, and other information related to patients' medical care.

The laptop computer was protected with a password, which provides a degree of protection against unauthorized access. However, passwords can be cracked, so there is a risk that information on the laptop could be viewed by unauthorized individuals. RAA of California said to date there has been no evidence found which indicates any of the information stored on the laptop computer has been accessed or misused.

Read entire article:
https://www.hipaajournal.com/stolen-laptop-contained-the-phi-of-dignity-health-patients/

NEWS

1 in 3 Americans Have Tried to Guess Someone's Password and 3/4 Succeeded

A recent study conducted on more than 1,000 Americans has revealed one in three Americans have attempted to guess someone else's password. Worryingly, in 73% of cases, that attempt to guess the password was successful.

Unsurprisingly, survey participants were most interested in guessing the password of a romantic partner, which accounted for 43.7% of attempts to guess a password. 40.2% of respondents said they attempted to guess the password of a parent. Worryingly, 21.7% of respondents said they had attempted to guess the password of a work colleague and 19.9% had attempted to guess the password of their boss.

The study, conducted by Beyond Identity on 1,015 individuals in the United States, provides insights into the password practices of Americans and confirms what security experts are all to aware of: People are bad at choosing passwords. Many people are aware how to create a strong password that is difficult to guess, but they still opt for a memorable password that they are unlikely to forget and it is common for passwords to consist of personal information that is known to others. 1 in 10 respondents to the survey thought their password could be guessed from looking at their social media profiles.

When asked about successful attempts to guess passwords, 39.2% of respondents said they guessed the password using information they knew about the person. 18.4% said they used information they found in social media profiles, 15.6% checked personal files or records, and 12.8% said they asked friends or loved ones for information. In 9.2% of cases, respondents were able to correctly guess the answer to a security question.

Read entire article:
https://www.hipaajournal.com/1-in-3-americans-have-tried-to-guess-someones-password-and-3-4-succeeded/

HIPAAQuiz

How can you prevent malicious software (malware) from harming your organization's network?

a. Install software *(e.g., music-sharing software, remote-access software, etc.)* only with approval from your organization's technical staff
b. Connect other devices *(e.g., laptop computers or personal digital assistants)* to the network only with approval from your organization's technical staff
c. Download antimalware tools to your computer
d. Both a and b

Answer: d
Software or hardware installed without the approval of your technical support department can cause security problems. Unapproved installations may disable your computer, threaten your organization's network, or contain malicious software that could allow access to someone not approved to see the information.

HIPAA Humor

"It used to be that if you worried about unseen forces you were considered paranoid. Now you're a security expert."

IN OTHER COMPLIANCE NEWS

LINK 1

Patients Sue DuPage Medical Group over July 2021 Ransomware Attack

https://www.hipaajournal.com/patients-sue-dupage-medical-group-over-july-2021-ransomware-attack/

LINK 2

TX: Denton County Discovers COVID-19 Application Leaked Data of 346,000 Individuals

https://www.hipaajournal.com/tx-denton-county-discovers-covid-19-application-leaked-data-of-346000-individuals/

LINK 3

Outpatient Facilities Targeted by Cyber Actors More Frequently Than Hospitals

https://www.hipaajournal.com/outpatient-facilities-targeted-by-cyber-actors-more-frequently-than-hospitals/

LINK 4

Health and Public Health Sector Warn of Elevated Risk of BlackMatter Ransomware Attack

https://www.hipaajournal.com/health-and-public-health-sector-warn-of-elevated-risk-of-blackmatter-ransomware-attack/

THUMBS UP to all MH Departments

for implementing awareness of…

HIPAA, PII, PHI, ePHI, Security, and Social Media

MIDLAND HEALTH

- *Main Campus*
- *West Campus*
- *Legends Park*
- *501a Locations*

Do you have exciting or interesting Compliance News to report?

Email an article or news link to:
Regenia Blackmon
Compliance Auditor
Regenia.Blackmon@midlandhealth.org