June 2020

COMPLIANCE CONNECTION

COMPLIANCE HOTLINE
877•780•9367

COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

DID YOU KNOW...

HIPAA Privacy Rule: Myths & Facts

Myth: HIPAA Prohibits Calling out Patients' Names *"Is there more personal information than an individual's name? Surely, HIPAA must discourage healthcare providers from calling their patients using their own names."*

Fact: The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure. The disclosure of a patient's identity to other patients in a waiting room is treated as one example of such incidental occurrences. Naturally, there still need to be reasonable safeguards to protect confidentiality and the purposes of such disclosure need to be strictly related to treatment. Certain types of treatment — such as psychiatry, fertility treatment, etc. — require additional focus on protection of confidentiality. This still, however, doesn't mean that HIPAA requires changing treatment or waiting areas to accommodate these regulations. You can also debunk this myth with the fact that Qminder has been HIPAA-certified, despite the use of visitor names being the central focus of its technology. Displaying names, especially when it's limited to first names and/or initials, does not breach the Privacy Rule — nor, for that matter, do sign-in logs, patient names on hospital doors, or publicly available treatment schedules.

Resource:
https://www.qminder.com/hipaa-myths-debunked/

FBI Issues Flash Alert About COVID-19 Phishing Scams Targeting Healthcare Providers

The FBI has issued a fresh warning following an increase in COVID-19 phishing scams targeting healthcare providers. In the alert, the FBI explains that network perimeter cybersecurity tools used by US-based healthcare providers started detecting COVID-19 phishing campaigns from both domestic and international IP addresses on March 18, 2020 and those campaigns are continuing.

These campaigns use malicious Microsoft Word documents, Visual Basic Scripts, 7-zip compressed files, JavaScript, and Microsoft Executables to gain a foothold in healthcare networks. While the full capabilities of the malicious code are not known, the FBI suggests that the purpose is to gain a foothold in the network to allow follow-on exploitation, persistence, and data exfiltration.

In the alert, the FBI provides indicators of compromise for the ongoing phishing campaigns to allow network defenders to take action to block the threats and protect their environments against attack.

In addition to taking steps to reduce risk, the FBI has requested healthcare providers who have been targeted in one of these COVID-19 phishing attacks to share copies of the emails they receive, including email attachments and full email headers. If any of the attacks are successful, the FBI has requested victims retain and share logs and images of infected devices, and perform memory capture of all affected equipment. That information can be used in the response by the FBI.

Read entire article:
https://www.hipaajournal.com/fbi-issues-flash-alert-about-covid-19-phishing-scams-targeting-healthcare-providers/

DID YOU KNOW...

Impermissible Disclosures of Protected Health Information

Any disclosure of protected health information that is not permitted under the HIPAA Privacy Rule can attract a financial penalty. This violation category includes disclosing PHI to a patient's employer, potential disclosures following the theft or loss of unencrypted laptop computers, careless handling of PHI, disclosing PHI unnecessarily, not adhering to the 'minimum necessary' standard, and disclosures of PHI after patient authorizations have expired.

Resource: https://www.hipaajournal.com/common-hipaa-violations/

MIDLAND
HEALTH

NEWS

HHS' Office of Inspector General Proposes Rule for Civil Monetary Penalties for Information Blocking

The HHS' Office of inspector General (OIG) proposed a rule that amends civil monetary penalty rules to also cover information blocking.

"When implemented, the new CMPs for information blocking will be an important tool to ensure program integrity and the promised benefits of technology and data," said Christi A. Grimm, OIG Principal Deputy Inspector General.

OIG understands that during the COVID-19 public health emergency, healthcare organizations are focused on providing treatment and follow-up care to patients. OIG is fulfilling its obligations by publishing the new rule but is also trying to be as flexible as possible to minimize the burden on healthcare organizations on the front line dealing with the COVID-19 pandemic. OIG is seeking comment from healthcare organizations and industry stakeholders on when information blocking enforcement should begin.

OIG explained that all entities and individuals required to comply with the new information blocking regulations will be given time to achieve compliance before enforcement begins. OIG has proposed the earliest date for enforcement is the compliance date of the ONC Final Rule published on March 9, 2020 but has proposed a 60-day delay to enforcement due to the COVID-19 pandemic.

The proposed rule does not introduce any new requirements concerning information blocking, instead OIG will be incorporating the regulations published by the National Coordinator for Health Information Technology (ONC) in March, and will be using that rule as the basis for enforcing information blocking CMPs.

Read entire article:
https://www.hipaajournal.com/hhs-office-of-inspector-general-proposes-rule-for-civil-monetary-penalties-for-information-blocking/

NEWS

Phishing Attack at BJC HealthCare Impacts Patients at 19 Hospitals

BJC Healthcare has announced that the email accounts of three of its employees have been accessed by an unauthorized individual after the employees responded to phishing emails.

Suspicious activity was detected in the email accounts on March 6, 2020 and the accounts were immediately secured. A leading computer forensics firm was engaged to conduct an investigation which revealed the three accounts had only been accessed for a limited period of time on March 6. It was not possible to tell if patient data was viewed or obtained by the attacker.

A review of the accounts revealed they contained the data of patients at 19 BJC and affiliated hospitals. Protected health information in emails and attachments varied from patient to patient and may have included the following data elements:

Patients' names, medical record numbers, patient account numbers, dates of birth, and limited treatment and/or clinical information, which included provider names, visit dates, medications, diagnoses, and testing information. The health insurance information, Social Security numbers, and driver's license numbers of certain patients were also potentially compromised.

All patients affected by the breach will be notified by mail when the email account review is completed. Patients whose driver's license or Social Security number has potentially been compromised will be offered complimentary credit monitoring and identity theft protection services.

BJC HealthCare said additional security measures will be implemented to prevent incidents such as this in the future and staff will be retrained to help them identify and avoid suspicious emails.

Read entire article:
https://www.hipaajournal.com/phishing-attack-at-bjc-healthcare-impacts-patients-at-19-hospitals/

HIPAAQuiz

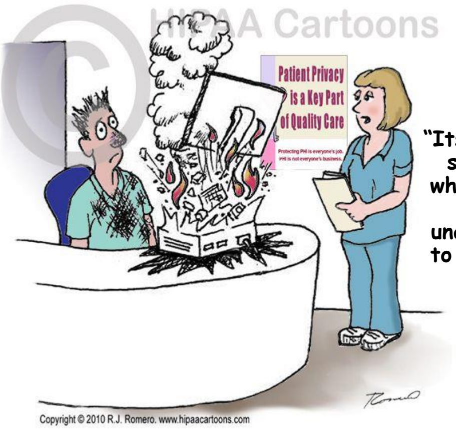
How can you prevent malicious software (malware) from harming your organization's network?

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

Reason: 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


HIPAA Cartoons
Patient Privacy is a Key Part of Quality Care
Protecting PHI is everyone's job. PHI is not everyone's business.
Copyright © 2010 R.J. Romero. www.hipaacartoons.com

"Its our new security software. That's what happens if the system detects unauthorized access to patient records."

IN OTHER COMPLIANCE NEWS

LINK 1

Senators Call for CISA and U.S. Cyber Command to Issue Healthcare-specific Cybersecurity Guidance

https://www.hipaajournal.com/senators-call-for-cisa-and-u-s-cyber-command-to-issue-healthcare-specific-cybersecurity-guidance/

LINK 2

HHS Delays Enforcement of New Interoperability and Information Sharing Rules

https://www.hipaajournal.com/hhs-delays-enforcement-of-new-interoperability-and-information-sharing-rules/

LINK 3

WHO Confirms Fivefold Increase in Cyberattacks on Its Staff

https://www.hipaajournal.com/who-confirms-fivefold-increase-in-cyberattacks-on-its-staff/

LINK 4

233,000 Patients Notified About PHI Breach at Genetic Testing Lab

https://www.hipaajournal.com/233000-patients-notified-about-phi-breach-at-genetic-testing-lab/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

Awareness of
HIPAA, PII, PHI, ePHI & 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