COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

FEATURE ARTICLE

HIPAA Quiz

(See Page 2 for Question & Answer)

DID YOU KNOW...

HIPAA privacy rule: Myths & Facts

Myth: *"In my practice, I use the NPP and I am careful about confidentiality, which makes me 'HIPAA compliant.'"*

Fact: Providers who have made real efforts at HIPAA compliance and experience a HIPAA violation may be fined as little as $100 if there's a violation. Those who have not made efforts towards compliance may be considered to have committed "willful neglect," which garners between $10,000-$50,000 in fines. The OCR is fairly forgiving to those who are compliant and experience a breach. However, those who don't attempt to be compliant and experience a breach will face a mandatory fine. The head-in-the-sand approach does not work when it comes to HIPAA. So, simply having an NPP in place and being "careful" does not make for HIPAA compliance. Providers must understand the rules around "use" and "disclosure" of PHI under the regulations and be sure patients are granted all of their privacy rights. A practice/organization must have completed a required security risk analysis that covers 54 standards and specifications under HIPAA; must have written HIPAA policies and procedures; and must train staff members/providers/volunteers on policies and procedures. Those who are unwilling or unable to facilitate a compliance program will fall into the camp of willful neglect. Under the regulations, providers cannot be sued by patients for lack of compliance, but there are other routes that may be taken should one be in violation of these regulations. For example, state attorneys general are enabled to sue for HIPAA violations. Additionally, patients have been able to successfully sue under tort law for violation of privacy.

Resource:
https://www.todayswoundclinic.com/blog/hipaa-privacy-security-compliance-dispelling-common-myths

Investigation Launched Over Snapchat Photo Sharing at M.M. Ewing Continuing Care Center

Snapchat

Certain employees of a Canandaigua, NY nursing home have been using their smartphones to take photographs and videos of at least one resident and have shared those images and videos with others on Snapchat – a violation of HIPAA and serious violation of patient privacy.

The privacy breaches occurred at Thompson Health's M.M. Ewing Continuing Care Center and involved multiple employees. Thompson Health has already taken action and has fired several workers over the violations. Now the New York Department of Health and the state attorney general's office have got involved and are conducting investigations.

The state attorney general's Deputy Press Secretary, Rachel Shippee confirmed to the Daily Messenger that an investigation has been launched, confirming "The Medicaid Fraud Control Unit's mission includes the protection of nursing home residents from abuse, neglect and mistreatment, including acts that violate a resident's rights to dignity and privacy."

Thompson Health does not believe the images/videos were shared publicly and sharing was restricted to a group of employees at the care center. Thompson Health is contacting the families of the residents impacted by the breach to offer an apology.

This is not the first time that Thomson Health has discovered an employee had taken pictures and videos without people's knowledge. In January, a camera was discovered in a unisex bathroom at Thompson Hospital. When the camera was taken down it was discovered that the memory card had been removed. The matter was reported to law enforcement although the employee responsible has not been identified.

M.M. Ewing Continuing Care Center is far from the only nursing home to discover that residents have been photographed and videoed without consent with videos and images shared on social media networks.

An investigation into the sharing of images of abuse of nursing home residents was launched by ProPublica in 2015. The investigation revealed the practice was commonplace, with several nursing home employees discovered to have performed similar acts. The investigation revealed there had been 22 cases of photo sharing on Snapchat and other social media platforms and 35 cases in total since 2012.

Read entire article:
https://www.hipaajournal.com/investigation-launched-over-snapchat-photo-sharing-at-m-m-ewing-continuing-care-center/

DID YOU KNOW...

Common HIPAA Violation:

"Failure to Use Encryption on Devices When Required by Company Policy"

Encryption includes measures to safeguard ePHI on portable devices. One of the most effective methods of preventing data breaches is to encrypt PHI. Breaches of encrypted PHI are not reportable security incidents unless the key to decrypt data is also stolen. Encryption is not required by HIPAA unless adopted by the covered entity.

MIDLAND HEALTH

New York Physician Notifies Patients of Exposure of their PHI

A New York physician has started notifying patients that their protected health information has been exposed and has been potentially accessed by unauthorized individuals.

Ruben U. Carvajal, MD was alerted to a possible privacy breach on January 3, 2018 and was informed that some of his patients' health information was accessible over the Internet. An investigation into the possible privacy breach was launched and the matter was reported to the New York Police Department and the Federal Bureau of Investigation (FBI).

FBI investigators visited his office and examined his computer. On February 18, 2018, the FBI confirmed that the EMR program on his computer had been accessed by an unauthorized individual. A forensic investigator was called in to conduct a thorough investigation to determine the nature and scope of the breach.

On May 22, 2018 the forensic investigator determined that the physician's computer had been accessed by an unauthorized individual between December 16, 2017 and January 3, 2018.

Any individual that gained access to the physicians' computer could have gained access to the EMR system, although the forensic investigation did not confirm whether the program was accessed, although based on the findings of the FBI it can be assumed that this was the case.

Read entire article:
https://www.hipaajournal.com/new-york-physician-notifies-patients-of-exposure-of-their-phi/

HIPAAQuiz

You need to talk to Mrs. Alberto about treatment options. There is another patient in the room and Mrs. Alberto's son is also there. Should you talk to Mrs. Alberto anyway, or wait until she is alone?

Answer: You should close the door and pull a curtain between the beds or use other parries to make the space as private as possible whenever you need to discuss health information with a patient. In general, you can reveal information to family members, but you should ask for the patient's consent first.

OCR Reminds Healthcare Organizations of HIPAA Rules for Disposing of Electronic Devices and Media

In its July Cybersecurity Newsletter, the Department of Health and Human Services' Office for Civil Rights has reminded HIPAA covered entities about HIPAA Rules for disposing of electronic devices and media.

Prior to electronic equipment being scrapped, decommissioned, returned to a leasing company or resold, all electronic protected health information (ePHI) on the devices must be disposed of in a secure manner.

HIPAA Rules for disposing of electronic devices cover all electronic devices capable of storing PHI, including desktop computers, laptops, servers, tablets, mobile phones, portable hard drives, zip drives, and other electronic storage devices such as CDs, DVDs, and backup tapes.

Healthcare organizations also need to be careful when disposing of other electronic equipment such as fax machines, photocopiers, and printers, many of which store data on internal hard drives. These devices in particular carry a high risk of a data breach at the end of life as they are not generally thought of as devices capable of storing ePHI.

If electronic devices are not disposed of securely and a data breach occurs, the costs to a healthcare organization can be considerable. Patients must be notified, it may be appropriate to pay for credit monitoring and identity theft protection services, and third-party breach response consultants, forensic investigators, and public relations consultants may need to be hired. OCR and/or state attorneys generals may conduct investigations and substantial financial penalties may be applied. Breach victims may also file lawsuits over the exposure of their financial information.

The costs all add up. The 2018 Cost of a Data Breach Study conducted by the Ponemon Institute/IBM Security highlighted the high cost of data breaches, in particular healthcare data breaches. The average cost of a breach of up to 100,000 records was determined to be $3.86 million. Healthcare data breaches cost an average of $408 per exposed record to mitigate, while the cost of data breaches of one million or more records was estimated to be between $40 million and $350 million.

It is not possible to ensure that all ePHI is disposed of securely if an organization does not know all systems and devices where PHI is stored. A full inventory of all equipment that stores ePHI must be created and maintained. When new equipment is purchased the list must be updated.

Read entire article:
https://www.hipaajournal.com/hipaa-rules-for-disposing-of-electronic-devices-and-media/

IN OTHER COMPLIANCE NEWS

LINK 1

OCR Reminds Healthcare Organizations of HIPAA Rules for Disposing of Electronic Devices and Media

https://www.hipaajournal.com/hipaa-rules-for-disposing-of-electronic-devices-and-media/

LINK 2

NIST/NCCoE Release Guide for Securing Electronic Health Records on Mobile Devices

https://www.hipaajournal.com/nist-nccoe-release-guide-for-securing-electronic-health-records-on-mobile-devices/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

MIDLAND HEALTH

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

A closer look at Protected Health Information (PHI)….

Remember, PHI is any health information an organization has or gets from another organization that could be used to identify a specific individual.

Know where PHI could be seen or heard by others.
Be aware of:

- *waste material that contains personal information about a patient, such as a used IV bag with a patient label on it*

Know where PHI could be seen or heard by others.
Be aware of:

- *computer monitors that could be seen by people passing by*

Know where PHI could be seen or heard by others.
Be aware of:

- *information you say aloud while talking to or about a patient*

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