COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

HIPAA privacy rule: Myths & Facts

Myth:

"All patients must acknowledge in writing they have received the HIPAA Notice of Privacy Practices (NPP)."

Fact:

Providers must provide patients with an NPP and attempt to get written acknowledgement that they've received notice. However, patients are not required to sign that they received the NPP. If they refuse to provide signature, the provider should document their refusal. Services cannot be denied based on a patient's refusal to provide a signature of acknowledgement of receipt of the NPP. It's important to understand the NPP does not take the place of informed consent for treatment, which typically lists the risks and benefits of treatment. The NPP solely covers patient rights and provider responsibilities.

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

Virginia Superior Court Partially Reverses Lower Court Decision in Employee Snooping Case

When healthcare employees access patient data without authorization it is a clear violation of the Health Insurance Portability and Accountability Act's Privacy Rule, but is the employer liable for the privacy breach?

In 2016, Lindsey Parker, a patient of Carilion Healthcare Corp's Carilion Clinic in Virginia, took legal action against the clinic and Carilion Healthcare Corp after it was discovered that two employees of the clinic had accessed her medical records and impermissibly disclosed a past diagnosis.

The privacy breach occurred in 2012 when Parker was a patient of the Carillion Rocky Mount Obstetrics & Gynecology clinic. Parker was visiting the clinic about a matter unrelated to her previous diagnosis and while waiting for treatment, Parker spoke with an acquaintance in the waiting room – Trevor Flava.

Parker alleged that a Carillion employee, Christy Davis, saw the couple talking and accessed Parker's medical record and saw her previous diagnosis. Davis is then alleged to have contacted her friend, Lindsey Young, who worked in another Carillion facility and disclosed the diagnosis and that Parker was conversing with Flava. Young then allegedly accessed Parker's record, confirmed the diagnosis, and disclosed that diagnosis to Flava.

Parker and her legal team sued Carilion Healthcare Corp, the Carilion Clinic, and both Carillion employees over the impermissible disclosure of her health information. In Parker's complaint it was alleged that Carillion was directly and vicariously liable for the breach – directly for the failure to secure her medical records and vicariously liable under respondeat superior principles. Parker also claimed that the breach amounted to negligence and a violation of HIPAA Rules for failing to ensure the confidentiality of her medical record. Parker also claimed the HIPAA violation also constituted a violation of Virginia law.

Read entire article:
https://www.hipaajournal.com/virginia-superior-court-partially-reverses-lower-court-decision-in-employee-snooping-case/

DID YOU KNOW...

Common HIPAA Violation:

"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.

MIDLAND HEALTH

Former Chilton Medical Center IT Worker Gets 5 Years Probation for Theft of Equipment Containing ePHI

A former IT worker at Chilton Medical Center in New Jersey has been sentenced to 5 years' probation for the theft of IT equipment that contained the protected health information of some of its patients.

Sergiu Jitcu, of Saddle Brook, NJ, had previously been employed by Chilton Medical Center. On October 31, 2017, Chilton Medical Center learned that one of its hard drives had been sold on eBay. The purchaser discovered databases on the hard drive that appeared to include the protected health information (PHI) of some of its patients.

The subsequent investigation revealed the hard drive contained the PHI of 4,600 patients who had received medical services at Chilton Medical Center between May 1, 2008 and October 15, 2017. The types of information on the hard drive included names, addresses, dates of birth, allergy information, medical record numbers, and medications.

The theft was reported to the Morris County Prosecutor's Office and was linked to Jitcu. The Morris County Prosecutor's Office Specialized Crime Division obtained a search warrant for Jitcu's home and vehicle and recovered computer equipment and additional items that had been stolen from Chilton Medical Center.

Jitcu was charged and plead guilty to one count of computer criminal activity and one count of theft of computer equipment. The offenses occurred between January 1, 2015 and November 8, 2017.

A non-custodial sentence of five years' probation was given to Jitcu on the condition that ongoing restitution payments be made to Chilton Medical Center totaling $64,250.

Read entire article:
https://www.hipaajournal.com/former-chilton-medical-center-it-worker-5-years-probation-theft-equipment-ephi/

HIPAAQuiz

People have taped their passwords to the wall near the patient database computer. Should you point this out to your supervisor?

Answer: Passwords should never be posted. If this happens, you should report this problem to your supervisor. Never post your password or share it with anyone else. If passwords have been made public, new passwords should be issued.

Altus Hospital Baytown Suffers Dharma Ransomware Attack

Altus Hospital in Baytown, TX, has experienced a ransomware attack that resulted in the encryption of many hospital records.

The electronic medical record system was not affected, although some of the encrypted files contained patients' protected health information including names, home addresses, contact telephone numbers, birth dates, Social Security numbers, credit card information, driver's license numbers, and medical information.

The attack was discovered on September 3, 2018. Altus Hospital received a ransom demand; however, assisted by a third-party security consultant, Altus Hospital was able to restore all affected files from backups.

The investigator determined that the attacker gained access to the hospital's servers before deploying a Dharma ransomware variant. Altus Hospital believes the aim of the attack was solely to extort money from the hospital. Data access and theft of patient information is not believed to have occurred.

While the attack was limited to Baytown hospital servers, some of the information stored on those servers came from the following affiliated entities: Altus Women's Center of Baytown, LP, LP, Clarus Imaging (Baytown), Oprex Surgery (Baytown), LP, Clarus Imaging (Beaumont), LP, Altus Radiation Oncology Baytown, LP, and Zerenity Baytown, LP.

Altus Hospital has retained external risk and security consultants who are helping to make improvements to the hospital's cybersecurity defenses.

PHI of 2,393 Patients of Southwest Washington Regional Surgery Center Compromised

Southwest Washington Regional Surgery Center has discovered an unauthorized individual has gained access to the email account of one of its employees as a result of a phishing attack.

The email account was breached on May 27, 2018 and access continued until August 13, 2018. Following an extensive forensic investigation of the breach and a manual review of all emails in the compromised account, Southwest Washington Regional Surgery Center determined on September 25 that the email account contained the protected health information of 2,393 of its patients.

The types of information that may have been accessed differed from patient to patient and may have included names, driver's license numbers, Social Security numbers, diagnoses, treatment information, details of surgical procedures performed, prescribed medications, lab test results, and health insurance information. Some patients' credit card numbers have also potentially been compromised.

Read entire article:
https://www.hipaajournal.com/altus-hospital-baytown-suffers-dharma-ransomware-attack/

IN OTHER COMPLIANCE NEWS

LINK 1

Billing Records of 12,331 Patients of Inova Health System Have Been Compromised

https://www.hipaajournal.com/billing-records-of-12331-patients-of-inova-health-system-have-been-compromised/

LINK 2

1,216 Patient Records Impermissibly Accessed by Former Upstate University Hospital Employee

https://www.hipaajournal.com/1216-patient-records-impermissibly-accessed-by-former-upstate-university-hospital-employee/

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.

The HIPAA Privacy Rule applies to most healthcare organizations that hold or transmit PHI:

- *hospitals*
- *healthcare provider offices*
- *providers of health insurance and HMOs (Health Maintenance Organizations)*

The HIPAA Privacy Rule applies to most healthcare organizations that hold or transmit PHI:

- *laboratories*
- *pharmacies*
- *radiology centers*

The HIPAA Privacy Rule applies to most healthcare organizations that hold or transmit PHI:

- *home-health agencies*
- *healthcare billing services*
- *clinics*

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