COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

FEATURE ARTICLE

HIPAA Quiz

#1 – An employer calls to see if a chronically ill employee was really at the doctor's office. Should you provide information about the patient?

#2 – A patient is leaving the pharmacy counter. You realize he forgot one of his medications and call out, "Mr. Jackson, you forgot your heart medication." Was that appropriate?

DID YOU KNOW...

HIPAA privacy rule: Myths & Facts

Myth: *"Members of the clergy can no longer find out whether members of their congregation or their religious affiliation are hospitalized unless they know the person by name."*

Fact: ***The Regulation specifically provides that hospitals may continue the practice of disclosing directory information "to members of the clergy," unless the patient has objected to such disclosure.*** Any requirement that the patient must list a specific church or any limitation on the practice of directly notifying clergy of admitted patients is either an internal hospital policy or based on a confused reading of the law.

$100,000 Settlement Shows HIPAA Obligations Don't End When a Business Closes

HIPAA covered entities and their business associates must abide by HIPAA Rules, yet when businesses close the HIPAA obligations do not end. The HHS' Office for Civil Rights (OCR) has made this clear with a $100,000 penalty for FileFax Inc., for violations that occurred after the business had ceased trading.

FileFax is a Northbrook, IL-based firm that offers medical record storage, maintenance, and delivery services for HIPAA covered entities. The firm ceased trading during the course of OCRs investigation into potential HIPAA violations.

An investigation was launched following an anonymous tip – received on February 10, 2015 – about an individual that had taken documents containing protected health information to a recycling facility and sold the paperwork.

That individual was a "dumpster diver", not an employee of FileFax. OCR determined that the woman had taken files to the recycling facility on February 6 and 9 and sold the paperwork to the recycling firm for cash. The paperwork, which included patients' medical records, was left unsecured at the recycling facility. In total, the records of 2,150 patients were included in the paperwork.

OCR determined that between January 28, 2015 and February 14, 2015, FileFax had impermissibly disclosed the PHI of 2,150 patients as a result of either: A) Leaving the records in an unlocked truck where they could be accessed by individuals unauthorized to view the information or; B) By granting permission to an individual to remove the PHI and leaving the unsecured paperwork outside its facility for the woman to collect.

Since FileFax is no longer in business – the firm was involuntarily dissolved by the Illinois Secretary of State on August 11, 2017 – the HIPAA penalty will be covered by the court appointed receiver, who liquidated the assets of FileFax and is holding the proceeds of that liquidation.

A corrective action plan has also been issued that requires the receiver to catalogue all remaining medical records and ensure the records are stored securely for the remainder of the retention period. Once that time period has elapsed, the receiver must ensure the records are securely and permanently destroyed in accordance with HIPAA Rules.

Read entire article:
https://www.hipaajournal.com/100000-settlement-filefax-ocr/

DID YOU KNOW...

Common HIPAA Violation:
Unprotected Storage of Private Health Information
A good example of this is a laptop that is stolen. Private information stored electronically needs to be stored on a secure device. This applies to a laptop, thumbnail drive, or any other mobile device.

MIDLAND HEALTH

Is a HIPAA Violation Grounds for Termination?

What actions are healthcare organizations likely to take if they discover and employee has violated HIPAA Rules?

Multiple HIPAA Failures Identified – Not all HIPAA violations are equal, although any violation of HIPAA Rules is a serious matter that warrants investigation and action by healthcare organizations.

When a HIPAA violation is reported – by an employee, colleague or patient – healthcare organizations will investigate the incident and will attempt to determine whether HIPAA laws were violated, and if so, how the violation occurred, the implications for patients whose privacy has been violated, potential legal issues arising from the violation and possible action by regulators. Healthcare organizations will be keen to take action to ensure that similar violations are prevented in the future. When an employee is discovered to have knowingly or unknowingly violated HIPAA Rules there are likely to be repercussions for the individual concerned. An unintentional acquisition, access, or use of protected health information by a workforce member in which the acquisition, access, or use was made in good faith and within the scope of authority would not be a reportable breach and may not necessarily result in disciplinary action.

Read entire article: https://www.hipaajournal.com/hipaa-violation-grounds-for-termination/

HIPAAQuiz

#1 – An employer calls to see if a chronically ill employee was really at the doctor's office. Should you provide information about the patient? *Generally you may not provide health information to outside parties without the authorization of the patient.*

#2 – A patient is leaving the pharmacy counter. You realize he forgot one of his medications and call out, "Mr. Jackson, you forgot your heart medication." Was that appropriate? *You should avoid using a patient's name in public. Never reveal information about a patient's medication or condition. You could say, "Excuse me sir, but you left one of your bags."*

Examples of HIPAA Violation Cases in Healthcare

Case #1: Facebook HIPAA Violation

In 2017, a HIPAA violation resulted in the firing of a medical employee after she posted about a patient on Facebook. The 24 year old med tech commented on a post about a patient killed in a car crash, using the words, "Should have worn her seatbelt…" While the comment itself seems innocent and even public-minded, it disclosed PHI about the patient. The employee later told reporters she was fired for a HIPAA violation, though the hospital declined to comment.

Case #2: Healthcare Worker Terminated in HIPAA Breach

A healthcare worker at a Washington State medical center was fired in 2017 for improperly accessing over 600 confidential patient health records. The medical center discovered the breach during a routine audit. The employee viewed information like addresses, phone numbers, diagnoses, and the social security numbers of patients.

Is Google Calendar HIPAA Compliant?

Google Is Google Calendar HIPAA compliant? Can the time management and calendar scheduling service be used by healthcare organizations or would use of the service be considered a violation of HIPAA Rules? This post explores whether Google supports HIPAA compliance for the Google Calendar service. Google Calendar was launched in 2006 and is part of Google's G Suite of products and services. Google Calendar could potentially be used for scheduling appointments, which may require protected health information to be added. Uploading any protected health information to the cloud is not permitted by the HIPAA Privacy Rule unless certain HIPAA requirements have first been satisfied.

A risk analysis must be conducted to assess potential risks to the confidentiality, integrity, and availability of ePHI. Risks must be subjected to a HIPAA-compliant risk management process and reduced to an acceptable level. Access controls must be implemented to ensure that ePHI can only be viewed by authorized individuals, appropriate security controls must be in place to prevent unauthorized disclosures, and an audit trail must be maintained. Further, healthcare organizations covered by HIPAA Rules are required to enter into a HIPAA-compliant business associate agreement with any vendor before any electronic protected health information is disclosed, even if the service provider says it does not access customer data. Google has appropriate security controls in place to protect data uploaded to Google Calendar and access and audit controls can be configured, so Google Calendar HIPAA compliance hinges on whether Google is willing to enter into a business associate agreement with HIPAA-covered entities or their business associates.

Google's Business Associate Agreement: Google is willing to sign a business associate agreement with healthcare organizations for its paid services, but not for any of its free services. The business associate agreement covers the use of G Suite, and includes Google Calendar, Google Drive, the chat messaging feature of Google Hangouts, Hangouts Meet, Google Keep, Google Cloud Search, Google Sites, Jamboard, and Google Vault services. HIPAA-covered entities must enter into a BAA with Google prior to any of the above services being used with ePHI.

Read entire article:
https://www.hipaajournal.com/google-calendar-hipaa-compliant/

IN OTHER COMPLIANCE NEWS

LINK 1

Hacking Responsible for 83% of Breached Healthcare Records in January

https://www.hipaajournal.com/hacking-responsible-83-breached-healthcare-records-january/

PHI Identifiers

Full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code that could be reasonably be associated with the individual

LINK 2

New York Surgery & Endoscopy Center Discovers 135,00-Record Data Breach

https://www.hipaajournal.com/new-york-surgery-endoscopy-center-discovers-135000-record-data-breach/

PHI Identifiers

Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

MIDLAND HEALTH

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

PHI Identifiers

Names; Phone numbers; Fax numbers; Social security numbers; Medical record numbers

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