COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

FEATURE ARTICLE

HIPAA Quiz

• You receive a call from an individual claiming that he or she is a friend of a patient and wants to inquire as to how the friend is doing. What information can you share?

DID YOU KNOW...

HIPAA privacy rule: Myths & Facts

Myth: *"Patients' medical records can no longer be used for marketing."*

Fact: ***Use or disclosure of medical information is explicitly permitted for certain health related marketing under the HIPAA Privacy Regulation.*** For example, communication about a plan's health related products or alternative treatments and services is not considered marketing for the purposes of the Rule-even if the health care provider is paid to encourage the patient to use the product or service. The 2000 version of the Privacy Rule required that patients be notified if the health care provider was paid to communicate about a health related product, be given the opportunity to opt out of future communications, and be informed of the identity of the source of the communication. The Bush Administration eliminated these safeguards from the Regulation.

Lawsuit Over HIPAA Breach by Mail Service Survives Motion to Dismiss

A mail service – Press America, Inc. – used by a pharmacy benefit manager – CVS Pharmacy – is being sued over an accidental disclosure of 41 individuals' protected health information.

CVS Pharmacy is a business associate of a health plan and is contracted to provide a mail-order pharmacy service for the health plan. The mail service is a subcontractor of CVS Pharmacy, and both entities are bound by HIPAA Rules.

CVS Pharmacy signed a business associate agreement with the health plan, and Press America did likewise with CVS Pharmacy as PHI was required in order to perform the mailings.

CVS Pharmacy alleges the HIPAA Privacy Rule was violated by Press America when it inadvertently disclosed PHI to unauthorized individuals due to a mismailing incident.

The disclosure of some plan members' PHI was accidental, but the privacy breach violated a performance standard in the CVS Pharmacy's contract with the health plan. By violating the performance standard, the CVS Pharmacy was required to pay the health plan $1.8 million.

A lawsuit was filed by the CVS Pharmacy seeking indemnification from the mail service under the terms of its BAA and common law principles. CVS Pharmacy alleges the mismailing was due to negligence by its subcontractor, and the $1.8 payment was made as a direct result of that negligence. CVS Pharmacy maintains the breach was fully under the control of its subcontractor.

CVS Pharmacy alleged the mail service owed it a duty of reasonable care and that duty of care was breached. Since PHI was improperly disclosed and the HIPAA Privacy Rule was violated, CVS Pharmacy was required to send notifications to the 41 plan members, which the complainant claims caused damage its reputation.

The mail service sought to dismiss the claim of negligence, and in its motion to dismiss the lawsuit, challenged the validity of the contractual obligation CVS Pharmacy had to the health plan that required the $1.8 million payment. The mail service also contended that its indemnification provisions were not intended to cover this type of payment.

Read entire article:
https://www.hipaajournal.com/lawsuit-hipaa-breach-mail-service-survives-motion-dismiss/

DID YOU KNOW...

Common HIPAA Violation:
Failure to Adhere to the Authorization Date
Patients can set a date when their authorization expires. A violation would be releasing confidential records after that date.

MIDLAND HEALTH

$3.5 Million Settlement to Resolve HIPAA Violations That Contributed to Five Data Breaches

Multiple HIPAA Failures Identified – OCR launched an investigation into the breaches to establish whether they were the result of failures to comply with HIPAA Rules. The investigation revealed a catalogue of HIPAA failures. OCR established that the FMCNA covered entities had failed to conduct a comprehensive and accurate risk analysis to identify all potential risks to the confidentiality, integrity, and availability of ePHI: One of the most common areas of non-compliance with HIPAA Rules. If an accurate risk assessment is not performed, risks are likely to be missed and will therefore not be managed and reduced to an acceptable level. OCR also discovered the FMCNA covered entities had impermissibly disclosed the ePHI of many of its patients by providing access to PHI that is prohibited under the HIPAA Privacy Rule. Several other potential HIPAA violations were discovered at some of the FMCNA covered entities. FMC Magnolia Grove did not implement policies and procedures governing the receipt and removal of computer hardware and electronic storage devices containing ePHI from its facility, and neither the movement of those devices within its facility. FMC Magnolia Grove and FVC Augusta had not implemented encryption, or an equivalent, alternative control in its place, when such a measure was reasonable and appropriate given the risk of exposure of ePHI.

Read entire article: https://www.hipaajournal.com/3-5-million-settlement-hipaa-violations-five-data-breaches/

HIPAAQuiz

You receive a call from an individual claiming that he or she is a friend of a patient and wants to inquire as to how the friend is doing. What information can you share?

If the individual calling inquires about the patient by name, you may share the health information the patient has authorized for inclusion in the hospital directory (name, location and general condition). Should the individual asking for the patient by name be a member of the clergy, you may also share the patient's religious affiliation.

Examples of HIPAA Violation Cases in Healthcare

Case #1: Former Hospital Worker Charged with HIPAA Violation

A Texas hospital employee got an **18-month jail term** for wrongful disclosure of private patient medical information. The employee was arrested in Georgia and found to be in possession of medical records. Though the filing didn't say how many records he had, he was charged with wrongful disclosure of private health information for personal gain. Individual charges like this aren't common because most violations of HIPAA aren't intentional. This case should serve as a warning that lone individuals aren't immune to prosecution.

Case #2: Criminal HIPAA Conviction for Respiratory Therapist

An employee of a Hospital in Ohio, accessed 596 medical records in a 10-month period. The employee was authorized to view records as part of her job, but only for the patients she was treating. Allegedly, she viewed files for unrelated patients. She could face up to a year in jail if convicted.

Is Google Voice HIPAA Compliant?

Google Voice is a popular and convenient telephony service that includes voicemail, voicemail transcription to text, the ability to send text messages free of charge, and many other useful features. It is therefore unsurprising that many healthcare professionals would like to use the service at work, as well as for personal use. In order for a service to be used in healthcare in conjunction with any protected health information (PHI) it must be possible to use it in a HIPAA compliant way.

That means the service must be covered by the conduit exemption rule – which was introduced when the HIPAA Omnibus Final Rule came into effect – or it must incorporate a range of controls and safeguards to meet the requirements of the HIPAA Security Rule. As with SMS, faxing and email, Google Voice is not classed as a conduit which means that in order for Google Voice to be HIPAA compliant, the service would need to satisfy the requirements of the HIPAA Security Rule. There would need to be access and authentication controls, audit controls, integrity controls, and transmission security for messages sent through the service. Google would also need to ensure that any data stored on its servers are safeguarded to the standards demanded by HIPAA. HIPAA-covered entities would also need to receive satisfactory assurances that is the case, in the form of a HIPAA-compliant business associate agreement (BAA). Therefore, before Google Voice could be used in conjunction with any protected health information, the covered entity must obtain a BAA from Google.

Will Google Sign A BAA for Google Voice? Google is keen to encourage healthcare organizations to adopt its services, and is happy to sign a business associate agreement for G Suite, but Google does not include its free consumer services in that agreement. Google does not recommend businesses use its free consumer services for business use, as they have been developed specifically for consumers for personal use. Google Voice is a consumer product and is not included in G Suite, Google Apps, or Google Cloud and neither is it mentioned in its BAA. ***So is Google Voice HIPAA compliant?*** *No. Until such point that Google releases a version of Google Voice for businesses, and will include it in its business associate agreement, it should not be used by healthcare organizations or healthcare employees in a professional capacity. The use of Google Voice with any protected health information would be a violation of HIPAA Rules.*

Resource: https://www.hipaajournal.com/google-voice-hipaa-compliant/

IN OTHER COMPLIANCE NEWS

LINK 1

A Recent Survey Indicated That 20% of RNs Had Breaches of Patient Data at Their Organization

https://www.hipaajournal.com/20-rns-breaches-patient-data-organization/

PHI Identifier

Phone numbers, fax numbers, electronic mail addresses; medical record numbers; account numbers

LINK 2

Is Azure HIPAA Compliant? Can Microsoft's cloud services be used by HIPAA covered entities without violating HIPAA Rules?

https://www.hipaajournal.com/azure-hipaa-compliant/

PHI Identifier

Biometric identifiers, including fingerprint and voice prints; Certificate/license numbers

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

MIDLAND HEALTH

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

PHI Identifier

Health plan beneficiary numbers; device identifiers and serials 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