COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

HIPAA privacy rule: Myths & Facts

Myth: *"Expect a big OCR fine if an email meant for one doctor lands in the wrong physician's inbox."*

Fact:
An email with protected health information (PHI) accidentally sent to the wrong health provider is not likely to get doctors in trouble with the Office for Civil Rights. In the last 12 years, there have been 184,000 HIPAA-related complaints to OCR and only 55 resulted in financial settlements, according to research Ms. Savage conducted through the Department of Health & Human Services website. Of the 55 settlements, none were associated with PHI accidentally sent from one health provider to another, she said in an interview. "[The OCR] tends to seek fines for really eye-poppingly bad behavior," Ms. Savage said, not small-scale accidents. For example, OCR fined one hospital for including the name of a patient in a press release without patient permission. Another health professional was fined for repeated failures to encrypt their computer system. If a document with PHI does end up in the wrong inbox, Ms. Savage advises calling the receiver and asking that they immediately delete the email.

Resource:
https://www.the-hospitalist.org/hospitalist/article/172926/practice-management/5-hipaa-myths-digital-age

Smartwatch Data Act Introduced to Improve Privacy Protections for Consumer Health Data

The Stop Marketing And Revealing The Wearables And Trackers Consumer Health (Smartwatch) Data Act, has been introduced by Sens. Bill Cassidy, M.D., (R-Louisiana) and Jacky Rosen, (D-Nevada). The new legislation will ensure that health data collected through fitness trackers, smartwatches, and health apps cannot be sold or shared without consumer consent.

The Health Insurance Portability and Accountability Act (HIPAA) applies to health data collected, received, stored, maintained, or transmitted by HIPAA-covered entities and their business associates.

Some of the same information is collected, stored, and transmitted by fitness trackers, wearable devices, and health apps. That information can be used, shared, or sold, without consent. Consumers have no control over who can access their health data. The new legislation aims to address that privacy gap.

The bill prohibits the transfer, sale, sharing, or access to any non-anonymized consumer health information or other individually identifiable health information that is collected, recorded, or derived from personal consumer devices to domestic information brokers, other domestic entities, or entities based outside the United States unless consent has been obtained from the consumer.

Consumer devices are defined as "equipment, application software, or mechanism that has the primary function or capability to collect, store, or transmit consumer health information."

The Smartwatch Data Act applies to information about the health status of an individual, personal biometric information, and kinesthetic information collected directly through sensors or inputted manually into apps by consumers. The Smartwatch Data Act would treat all health data collected through apps, wearable devices, and trackers as protected health information. There have been calls for HIPAA to be extended to cover app developers and wearable device manufacturers that collect, store, maintain, process, or transmit consumer health information. The Smartwatch Data Act does not extend HIPAA to cover these companies, instead the legislation applies to the data itself. The bill proposes the HHS' Office for Civil Rights, the main enforcer of compliance with HIPAA, would also be responsible for enforcing compliance with the Smartwatch Data Act. The penalties for noncompliance with the Smartwatch Data Act would be the same as the penalties for HIPAA violations.

Read entire article:
https://www.hipaajournal.com/smartwatch-data-act-consumer-health-data/

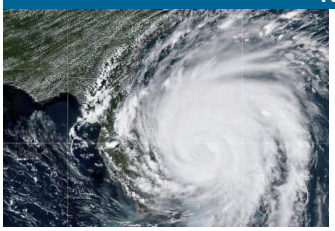
DID YOU KNOW...

Proper Disposal of PHI

When physical PHI and ePHI are no longer required and retention periods have expired, HIPAA Rules require the information to be securely and permanently destroyed. For paper records this could involve shredding or pulping and for ePHI, degaussing, securely wiping, or destroying the electronic devices on which the ePHI is stored to prevent impermissible disclosures.

MIDLAND HEALTH

NEWS



Hurricane Dorian: Limited HIPAA Waiver Issued in Puerto Rico, Florida, Georgia, North and South Carolina

Alex Azar, Secretary of the Department of Health and Human Services (HHS), has declared a public health emergency (PHE) in Puerto Rico and the states of Florida, Georgia, and South Carolina due to Hurricane Dorian. On September 4, a PHE was also declared in North Carolina, retroactive to September 1, 2019.

The announcement follows the presidential PHE in the above areas as the states prepare for when the hurricane makes landfall. The declaration was accompanied by the announcement of a limited waiver of HIPAA sanctions and penalties for certain provisions of the HIPAA Privacy Rule, as mandated by the Project Bioshield Act of 2004 of the Social Security Act. The waiver only applies in the emergency areas and for the period of time covered by the PHE.

The waiver applies to hospitals that have implemented their disaster protocol, and only for up to 72 hours from when the disaster protocol was implemented, unless the PHE declaration terminates before that 72-hour period has elapsed.

Once the PHE comes to an end, hospitals are required to comply with all requirements of the HIPAA Privacy Rule for all patients, including those still under the care of the hospital when the PHE ends. The HHS notes that during a PHE, the requirements of the HIPAA Privacy and Security Rules remain in place.

Even in the absence of a HIPAA waiver, the HIPAA Privacy Rule permits the sharing of patient information with friends, family, public health officials, and emergency personnel. Entities can share patient information for the purposes of providing treatment, for public health activities, and to lessen a serious threat to public health or safety. Information can also be shared with patients' friends, family and other individuals involved in their care to ensure that proper care and treatment can be provided.

Read entire article:
https://www.hipaajournal.com/hurricane-dorian-limited-hipaa-waiver-issued-in-puerto-rico-florida-georgia-south-carolina/

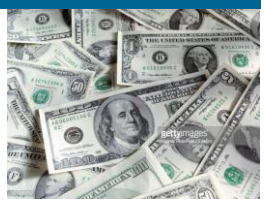
HIPAAQuiz

How does HIPAA define a healthcare clearinghouse?

Answer: *Under HIPAA, a healthcare clearinghouse is a Covered Entity that processes or facilitates processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. A healthcare clearinghouse would typically receive a standard transaction from another entity and process or facilitate the processing of health information into nonstandard format or nonstandard data content for the receiving entity.*

NEWS

How Much Does HIPAA Compliance Cost?



By: Jen Stone
Security Analyst
CISSP, QSA, CISA, CCSFP

Realistic HIPAA security budgets vs. wishful thinking:

HIPAA compliance is rarely allocated the resources it requires. And this trend extends beyond just small organizations with limited security budgets. Lack of budget is a plague that affects risk and compliance officers at health organizations of all sizes.

This post will give you the information you need to more accurately plan your HIPAA budget.

What does the HHS think HIPAA compliance costs?

The HHS gave an interesting estimation of how much HIPAA compliance might cost, shortly after they released the HIPAA Final Rule in 2013.

Per organization, they estimated:

- **$80** for an updated Notice of Privacy Practices
- **$763** for breach notification requirement updates
- **$84** for business associate agreement updates
- **$113** for security rule compliance

Grand total per organization: **$1,040**

This estimate is likely inaccurate, especially when considering the complexities of the Security Rule. When the Security Rule was added back in 2003, it included 75 new requirements and 254 points for organizations to validate most of which are quite technical.

Resource:
https://www.securitymetrics.com/blog/how-much-does-hipaa-compliance-cost#.XdV3rlB2WM8.email

HIPAA Humor

IN OTHER COMPLIANCE NEWS

LINK 1

Two Maine Healthcare Providers Report Email Security Breaches Impacting 52,000 Patients

https://www.hipaajournal.com/two-maine-healthcare-providers-report-email-security-breaches-impacting-52000-patients/

LINK 2

Texas Health and Human Services Commission Pays $1.6 Million HIPAA Penalty

https://www.hipaajournal.com/texas-health-and-human-services-commission-pays-1-6-million-hipaa-penalty/

LINK 3

HHS Increases Civil Monetary Penalties for HIPAA Violations in Line with Inflation

https://www.hipaajournal.com/hhs-increases-civil-monetary-penalties-for-hipaa-violations-2019-inflation/

LINK 4

Speakap Confirmed as HIPAA Compliant by Compliancy Group

https://www.hipaajournal.com/speakap-confirmed-as-hipaa-compliant-by-compliancy-group/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

MIDLAND HEALTH

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