Department of Mental Health and Addiction Services | Office of the Commissioner | Elizabeth Taylor, Chief Compliance Officer

Fall 2017

COMPLIANCE CONNECTION

INSIDE THIS ISSUE:

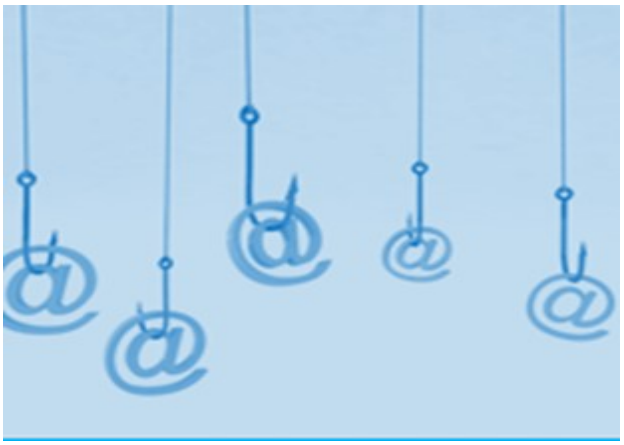
"Individuals cannot trust in a health care system that does not appropriately safeguard their most sensitive PHI," said Roger Severino, OCR director."Covered entities and business associates have the responsibility under HIPAA to both identify and actually implement these safeguards."

Anyone Phishing Lately?

Did you know that phishing is the number one attack vector for gaining access to sensitive data and delivering malware to our systems?

Information captured through phishing can be used to commit identity theft, medical insurance fraud and other malicious activities. Gaining information through phishing allows the bad actor to create new identities, fraudulent credit card accounts, and access into a person's insurance plan information.

Medical fraud (or PHI) is one of the most desired forms of fraudulent information for bad actors to gain. While credit card information is still a desired commodity, phishing for medical record (PHI) information is on the rise.



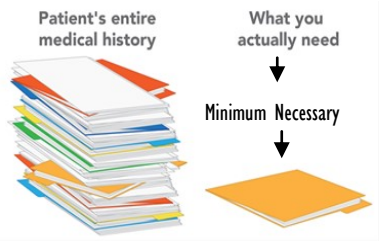
Why do criminals want PHI?

Your banking and credit card information (once discovered) has an "end date" and can be quickly shut down. The medical record information (PHI) can be used, sold, created and recreated in a number of ways. It contains our medical history, diagnoses, pharmacy, medications, address and so on.

All DMHAS workforce must be vigilant and safeguard our clients' right to privacy, confidentiality and PHI (medical record) information at all times. ***Do not include PHI in email*** — and if you receive an email from an entity that you don't readily recognize (or it's asking you to provide information) — STOP — before you click on that link. ***Someone could be phishing!!***

MINIMUM NECESSARY STANDARD

The Minimum Necessary Standard of the HIPAA Privacy Rule tells us that we should not only protect and safeguard our clients' PHI, but share only what is necessary. What does that mean – and how do you know what constitutes "minimum?"



The minimum necessary standard requires covered entities (that's us) to limit the use or disclosure of (and requests for) protected health information (PHI) to the minimum necessary to accomplish the intended purpose. That means only accessing and using what is needed to do your job. It means disclosing only the portion of the medical record that is necessary .

If you are not sure what you may or may not share and disclose – please contact me or your facility compliance officer - - we're here to help!

While the HIPAA Breach Notification Rule allows covered entities 60 days following the discovery of a breach entities must report "without unreasonable delay…"

Compliance means doing the right thing.

"There are no easy answers, but there are simple answers. We must have the courage to do what we know is morally right."

News you can Use . . .

Misdirected fax costs $387,200

In September 2014, the HHS Office for Civil Rights (OCR) received a complaint alleging that a staff member had impermissibly disclosed PHI to the patient's employer. The patient was receiving treatment at the Center which included HIV status, and behavioral health information. St. Luke's-Roosevelt Hospital Center Inc, is 1 of 7 hospitals that comprise the Mount Sinai Health System (MSHS).

The patient had previously requested the Center send his PHI to a personal post office box; however a Center employee mistakenly faxed the PHI to the patient's employer .

After receiving the compliant, OCR investigators discovered that a similar breach had occurred at the Center nine months before when a staff member faxed a patient's PHI to an organization at which he volunteered.

Despite the misdirected fax, the Center failed to address the vulnerabilities in their operations and compliance program to prevent a similar incident from occurring again. This fax to the patient's employer was the second such incident for which the Center had impermissibly disclosed PHI. These two misdirected faxes cost a New York City hospital $387,200 in a HIPAA settlement.

What you need to know

Be sure you have a valid consent (release of information) before disclosing PHI. Double-check the fax number and ensure the receiving entity is correct and permissible. Have you checked your auto-fax numbers recently to ensure they haven't changed?

Delayed HIPAA Breach Notification costs $475,000

Presense Surgery Center at St. Joseph Medical Center in Joliet, Illinois, experienced a physical breach of PHI October 2013. It was discovered that operating room schedules had been removed from the surgery center and could not be located. The documents contained sensitive information on 836 patients that included their name, date of birth, medical record number and details of the procedures, dates etc. that were performed. The surgery center reported the breach to OCR 104 days after the breach was discovered. The Breach Notification Rule requires reporting within 60 days or "without unreasonable delay." The surgery center was noted to have reported the breach 31 days after the Rule deadline had passed. While investigating, OCR noted that Presense Health had experienced smaller breaches in 2015 and 2016 yet failed to provide affected individuals with timely breach notifications.

What does this mean for us?

If you discover (or believe) there is breach of PHI, make sure you notify your facility compliance officer or the chief compliance officer immediately. And remember to use a secure, locked bag if you must transport PHI!

References

https://www.hhs.gov/about/news/2017/05/23/careless-handling-hiv-information-costs-entity.html

https://www.healthleadersmedia/technology/misdirected-fax-cost-hospital-387200

https://www.hipaajournal.com/mjhs-phishing-attack-result-exposure-28000-individuals-phi-8938/

Quote: Ronald Reagan

Chief Compliance Officer:

Elizabeth Taylor, OOC,
860.418.6648

Do you have a topic of particular interest you would like to know more about? If so, please contact me (above) or send an email to elizabeth.taylor@ct.gov

Facility Compliance Officers:

Ellen Brotherton, WCMHN
Tracey Edwards, SMHA
Megan Goodfield, RVS
Gretchen Mrozinski, CMHC
Marlana Rugg, CRMHC
Paula Zwally, SCMHS

To report anonymously:
Toll free: 877.277.9471

Compliance Hotline: 860.418.6991
Privacy Hotline: 860.418.6901