Published on *University of Colorado* (https://www.cu.edu)

HIPAA and Knowing Your Audience [1]

When sharing personally identifiable information (PII) and protected health information (PHI), get in the habit of thinking about your audience twofold: *who is the subject and who is the recipient?*

Information should only be shared on a *need to know basis personally and legally* with the mindset that the sender/creator has the responsibility to respect and protect an individual's right to privacy.

Protecting PHI/PII is the intent behind the governing federal law, the Health Insurance Portability and Accountability Act (HIPAA). Compliance with HIPAA by way of effective management, security controls, privacy rules and proper intake of PHI/PII, safeguards a person's information. Those who properly work to secure such information uphold a strong security and privacy culture across an organization. A strong security and privacy culture can protect organizations from bad PR, fines and penalties. As an example, regarding legal and personal privacy expectations look at the characters Carmen Sandiego and Batman. Both need to have their PII- identifiable information [2] protected for different reasons in regards to HIPAA.

Where is

Address
Ip Address
Vehicle identifiers (serial numbers, license plates)

Carmen Sandiego?

Legal Name

Carmen Sandiego, an international espionage extraordinaire, has prolonged being captured since the early 90s by concealing important parts of her PII. With her in mind, we know that most of our potential audience only knows her identity. Therefore, when the sender is drafting an email about Carmen's (the subject) medical record to a potential tracker (the recipient), great care should be taken to not include her geographical information as that is her wish and this identifier is protected under HIPAA.

Who

Social Security Number
Biometric identifiers
Full face photographic images
Birth date
Age

Is The Batman?

Legal Name

Batman, aka Bruce Wayne, spotlights as the cape crusader to carry out acts of vigilante justice. For Batman, concealing his identity is vital to this mission as it strengthens his authority in the mind of potential criminals. With Batman in mind, his primary care doctor will avoid sending his social security number to random people as that would be against the Bat's wishes and this identifier is protected under HIPAA.

Long story short, disclosing a combination of too much PHI and PII is risky for the subject and for the organization securing this data. Organizations can use PHI and PII as it relates to payment, treatment, and operations. However, users within the organization should not become comfortable within their environment. The process of knowing your audience and implementing safeguards to protect PII/PHI can be quite difficult and is on-going. Please see below for examples of technical, administrative, and physical safeguards.

Technical Safeguards

Outlook

- Create folders and rules for emails involving PII/PHI.
- Double check the To and CC /BCC fields before sending any email.
- Do not use Outlook as your primary source for file storage. Archive your mailbox
- Set your Outlook Contact List to be locked. Private
- Do not store all the 18 personal identifiers for a contact in Outlook.
- Only share your contact list with recipients on a need to know basis.
- Do not take the bait by way of phishing. If an email looks suspect it probably is. Contact your Campus OIT regarding suspicious emails.

Word

- Encrypt the document with a password.

Excel

- Accordingly hide and protect rows/columns that contain sensitive University Information/PII/PHI.

- Encrypt the workbook with a password.

Cloud Storage

- Contact your IT department [3]for campus-specific requirements when sending files/storing files that contain sensitive PII/PHI.

Social/Collaborative

- Be cautious about the collaborative applications that you use to share sensitive University information-PII-PHI. Each collaborative application is built differently, and some are not vetted as being HIPAA compliant.
- Do not rely on any collaborative application as your primary application for data storage.

Other Applications

- If you are unsure about an application or service, please reach out to your campus OIT to conduct an application assessment before purchasing/implementing it.

General

- The first defense is always your password. Create a strong password by exceeding the password requirements for any site/application. Additionally, do not use the same password for every site.

Administrative Safeguards

- CU departments/units should create an acceptable use policy for applications that their department frequently uses.
- CU departments who work with PII/PHI data should implement their own internal HIPAA awareness/ security training.

Physical Safeguards

- Double check who you are speaking to--verbally and in writing. Are they wearing a CU badge? Is their email address a CU email address?
- Do not minimize the process of badging into a secure area for the sake of politeness. Do not let other people badge in under your authorized access and do not hold doors open for secure areas.

By Angela Harris and Richard Akoto, University of Colorado Denver | Anschutz Medical Campus

Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/hipaa-and-knowing-your-audience
[2] https://research.cuanschutz.edu/regulatory-compliance/home/hipaa/protected-health-information-(phi)
[3] https://www.cu.edu/security/about