Provider Role in Protecting Patient Confidentiality, Privacy, and Security Beyond HIPAA

AHIMA continues to advocate for privacy protections to ensure the patient-provider trust bond is preserved and patient confidentiality, privacy and security is protected. In absence of a national privacy law, much of the responsibility for educating patients on how to protect their data in non-HIPAA covered environments falls on the provider organizations. HI professionals can utilize the below resources to assist in navigating conversations on data confidentiality, privacy and security.

Understanding the Current Public Policy Landscape:

US Department of Health and Human Services (HHS) Office for Civil Rights (OCR): Health App Use Scenarios & HIPAA (available here)

- A tool that outlines how HIPAA Rules apply when working with third-party health apps.

Education responsibilities under the HHS Office of the National Coordinator for Health Information Technology (ONC) information blocking policies (available here)

- Page 25815 of the ONC information blocking final rule "strongly encourages [providers] to provide individuals with information that will assist them in making the best choice for themselves in selecting a third-party application."
    - If a patient decides to use a third-party app, even if a provider actor has determined it is not secure, a provider under information blocking is not allowed to prevent or limit the amount of information sent to that app at the patient's request.

Patient Focused Tools:

Think Before You Click patient focused resources (available here)

- A CHIME and WEDI developed resource to assist consumers looking to share their health information with non-HIPAA covered apps and considerations they should take before sharing.

US Department of Health and Human Services (HHS) Office for Civil Rights (OCR): Protecting the Privacy and Security of Your Health Information When using Your Personal Cell Phone or Tablet (available here)

- HHS guidance detailing how patients can keep their location and activity private and contains links to many other tools on increasing privacy.

Federal Trade Commission (FTC): How to Protect Your Privacy on Apps (available here)

- Guidance for users on how to protect their privacy when using apps on their mobile device.

Office of the National Coordinator for Health Information Technology (ONC): How Can You Protect and Secure Health Information When Using a Mobile Device? (available here)

- Tools for patients to protect and secure their information when navigating the mobile technology space.

Federal Reporting Resources:

If a patient suspects their privacy or data was illegally compromised or mishandled by a non-HIPAA covered entity they should contact the FTC at https://consumer.ftc.gov/.

Questions?

If you have questions about the current privacy environment or these resources, please contact the AHIMA Policy & Government Affairs team at advocacy@ahima.org.

Updated: July 2022