HOW TO PROTECT YOUR HEALTH INFORMATION

Steps you should consider taking to help protect the privacy and security of your health information:

If you store health information, including substance use disorder (SUD), or addiction treatment information, on your personal computer or mobile device, exchange emails about it, or participate in health-related online communities, here are a few things you should know:[i]

- **The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules are in place to protect and secure your health information.**
  - These protections must be followed by your health care provider (such as your doctor or hospital) and your health insurance company.
  - However, the laws do not apply if you share your health information with an organization that is not covered by HIPAA!
    - For example, if you post your health, including SUD treatment, information online — like on a message board about a health condition, it is not protected by HIPAA.
  - *Never post anything online that you don't want made public.*

- **Your SUD (or other health) provider uses tools to protect and secure your health information at their office. You can do the same at home.**
  - Passwords can help keep your information safe.
  - If you have health information stored on your home computer or mobile device — or if you discuss your health information over email — simple tools like passwords can help keep your health information secure if your computer is lost or stolen.

- **There are medical identity thieves that could try to use your personal and health insurance information to get medical treatment (including SUD treatment), prescription drugs, or surgery.**
  - The best way to protect yourself is to make sure you verify the source before sharing your personal or medical information.
  - Safeguard your medical and health insurance information and shred any insurance forms, prescriptions, or physician statements.
  - For more information about medical identity theft, visit the Federal Trade Commission (FTC) website to learn how to protect yourself.

- **If you store your health information online, you should be sure to read the website's privacy policy and terms of service.**

Here are more steps you can take to protect and secure your health information online.

- **Most websites convert information or data into a code to protect your health information and prevent unauthorized access.**
  - This conversion process is known as encryption.
  - Always look for a lock symbol or “https” in the address bar to the left of the website address to ensure that your connection is encrypted.

- **Make sure your security software, operating system, and internet browser are up to date.**
  - Update your phone's operating system, as well and turn on automatic updates to keep up with the latest protections.

- **Create a strong password that's hard to guess.**
  - Start by making your password long, aim for at least 12 characters.
  - If the account doesn't allow long passwords, mix uppercase and lowercase letters, numbers, and symbols to make your password stronger.
  - Turn on two-factor authentication when it is available.

- **Pick security questions only you can answer.**
  - When you create an account, you may have to give answers to a few security questions. Some sites may periodically ask you to answer these questions as a security measure to confirm your identity.
  - You also may have to answer them if you need to reset your password.
  - Avoid questions with a limited number of responses that hackers can guess like the color of your first car.
  - Skip questions with answers that someone could find online or in public records — like your zip code, birthplace, or mother's maiden name.
  - If you can't avoid those questions, treat them like a password and use random and long answers. Just be sure you can remember your answers.
  - As with a password, make sure the question and answer are unique, not one that you use on other sites.

- **If you use your cell phone to access sensitive personal information set your phone to lock when you're not using it and create a PIN or passcode to unlock it.**
  - Use at least a 6-digit passcode. You also might be able to unlock your phone with your fingerprint, your retina, or your face.

- **Look for unusual behavior from your phone, tablet, or computer.** Your device might have been infected with malware if it:
  - suddenly slows down, crashes, or displays repeated error messages.
  - won't shut down or restart.
  - won't let you remove software.
  - serves up lots of pop-ups, inappropriate ads, or ads that interfere with page content.
  - shows ads in places you typically wouldn't see them, like government websites.
  - shows new and unexpected toolbars or icons in your browser or on your desktop.
  - uses a new default search engine or displays new tabs or websites you didn't open.
  - keeps changing your computer's internet home page.
  - sends emails you didn't write.
  - runs out of battery life more quickly than it should.

- **Recognize scammers**.
  - Scammers pretend to be someone they're not, like a representative from a well-known company or the government, to rip you off or steal your personal information.
  - They also create fake websites and encrypt them to make you think they're safe when they're not.
  - If you visit a scammer's website, your data may be encrypted on its way to the site, but it won't be safe from scammers operating the site.
  - If you visit a scammer's website or receive a call from a scammer report the incident to the FTC at ReportFraud.ftc.gov.

What to consider when selecting an application to retrieve protected health care information.

When authorizing a third-party app to retrieve your health care data (including SUD treatment) it is important for you to take an active role in protecting your health information. Below are things to look for when choosing an app to retrieve your protected health care data.

You should consider:
○ What health data will this app collect? Will this app collect non-health data from my device, such as my location? ○ Will my data be stored in a de-identified or anonymized form? ○ How will this app use my data? ○ Will this app disclose my data to third parties? ▪ Will this app sell my data for any reason, such as advertising or research? ▪ Will this app share my data for any reason? If so, with whom? For what purpose? ○ How can I limit this app's use and disclosure of my data? ○ What security measures does this app use to protect my data? ○ What impact could sharing my data with this app have on others, such as my family members? ○ How can I access my data and correct inaccuracies in data retrieved by this app? ○ Does this app have a process for collecting and responding to user complaints? ○ If I no longer want to use this app, or if I no longer want this app to have access to my health information, how do I terminate the app's access to my data? ○ If I no longer want to use this app, or if I no longer want this app to have access to my health information, how do I terminate the app's access to my data? ○ What is the app's policy for deleting my data once I terminate access? Do I have to do more than just delete the app from my device? ○ How does this app inform users of changes that could affect its privacy practices?

If the app's privacy policy does not clearly answer these questions, patients should reconsider using the app to access their health information. Health information is very sensitive information, and patients should be careful to choose apps with strong privacy and security standards to protect it.

How to File a Complaint

If you believe your information was used or shared in a way that is not allowed under the HIPAA Rules, or if you were not able to exercise your rights, you can file a complaint with the facility where you obtain health care or any of the offices listed below.

County of Los Angeles

Department of Public Health

Privacy Officer
1000 S. Fremont Ave.
A9E, 5th Floor - South
Alhambra, CA 91803
(888) 228-9064

You may also file a complaint with the **U.S. Department of Health and Human Services**

Office for Civil Rights at (800) 368-1019 (TDD: 800-537-7697) or by sending a letter to:

Region IX, Office for Civil Rights
U.S. Department of Health and Human Services
90 7th St. Suite 4-100
San Francisco, CA 94103

You may also file a complaint at this link: www.hhs.gov/ocr/privacy/hipaa/complaints/

If you believe that a company that is not covered by HIPAA, such as a message board, life insurance company, employer, workers' compensation carrier, school or school district, state agency not related to healthcare such as law enforcement, child protective services or a wearable tech company has shared your health information in a way that conflicts with their privacy policy on their website, you can file a complaint with the Federal Trade Commission.

How to file a complaint with The Federal Trade Commission

You can file a complaint online at ReportFraud.ftc.gov or by calling 1-877-FTC-HELP (1-877-382-4357).

Report A Breach

You can also email the FTC at Healthbreach@ftc.gov or call (202) 326-2918 to report a health data breach.

[i] (Health IT, Privacy, Security and HIPPA, 2017)https://www.healthit.gov/topic/privacy-security-and-hipaa/what-you-can-do-protect-your-health-information

[ii] (Federal Trade Commission Consumer Advice, Online Privacy and Security, 2023)https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security