Protecting the Privacy and Security of Your Health Information

The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules protect the privacy and security of your medical and other health information when it is transmitted or maintained by covered entities and business associates. This information is referred to as Protected Health Information (PHI), and it includes individually identifying information, such as your name, address, age, Social Security Number (SSN), and location, as well as information about your health history, any diagnoses or conditions, current health status, and more.

HIPAA covered entities

These include any organization or person that transmits data around payment transactions for medical treatment or insurance. San Joaquin County Behavioral Health Services (SJCBHS) is subject to HIPAA. Additional details are available at

- https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

HIPAA non-covered entities

These are entities who are not healthcare providers, healthcare clearinghouses, or health plans; however, they often store health related information and may still have to comply with other aspects of HIPAA:

- Wearable technology, for example smart watches, sleep monitors
- Health apps
- Providers who do not deal with electronic data

The HIPAA rules generally **do not** protect the privacy or security of your health information when it is accessed through, or stored, on your personal devices (for example, cell phones, tablets). HIPAA rules **do not** protect the privacy of data you download or enter into third-party applications for your personal use, regardless of where the information came from.

Sharing Your Health Information

SJCBHS currently participates in the California Mental Health Services Authority (CalMHSA) electronic health record system. CalMHSA has built CalMHSA Connex, a specialized platform designed for seamless and secure sharing of behavioral health information among diverse health care entities, including facilitation patient access to their data. This exchange:

- Is tailored to the needs of mental health and substance use disorder treatment providers
- Enables the confidential transmission of patient records, treatment plans, and outcomes across the behavioral health spectrum
- Emphasizes privacy and consent management and ensures that sensitive information is shared only with authorized individuals, fostering collaborative and comprehensive care

To opt out of SJCBHS sharing your information with CalMHSA Connex, download and complete the patient non-participation form BHSHIE Opt out form

To opt out of data sharing in CalMHSA Connex completely, download and complete the form on the CalMHSA webpage https://www.calmhsa.org/interoperability-optout/

Privacy and Security of Your Health Information When Selecting and Using Third-Party Applications (Apps)

You have the right to request your health information be sent to electronic devices, including apps. Most apps **are not** covered by HIPAA. By law, SJCBHS cannot recommend or offer an opinion on any third-party apps. It is important that you understand the security and privacy practices of any application you entrust with your health information. You can increase the privacy of your information when using your personal devices:

- Avoid downloading unnecessary or random apps
- Avoid sharing your device's location data unless necessary (manage the location services on your device through settings). For information about data privacy on your device:
    - https://www.apple.com/privacy/control
    - https://www.android.com/safety
- Manage the information shared with apps through the app settings. For details of how to protect your privacy when using apps, or to see reviews of data practices of electronic products, visit:
    - https://consumer.ftc.gov/articles/how-protect-your-privacy-apps
    - https://www.consumerreports.org/issue/data-privacy
- Use apps that have an increased focus on privacy and security:
    - Use strong encryption by default when transmitting data
    - Enable technology to limit or block tracking tools such as cookies or web trackers
    - Do not collect and store personal information
- Consider what health data an app collects and whether the data is de-identified or anonymized. Be familiar with what information is collected and used.
    - https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information
- Delete stored data on devices before disposing of them
- Understand how to delete an app's access to your data and what the app policy is for deleting your personal data.

Reporting Privacy Related Complaints

The U.S. Department of Health and Human Services (HHS) office for civil rights is responsible for enforcing HIPPA rules related to covered entities and provides guidance on their website.

- https://www.hhs.gov/hipaa/filing-a-complaint/index.html
- https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf

The Federal Trade Commission (FTC) covers apps. Protections against deceptive acts, for example an app shares personal information without your permission in violation if the app's privacy policy, are covered under the FTC Act.

- https://reportfraud.ftc.gov/#/

Filing a complaint with SJCBHS

- In person by completing the grievance form and providing it to an employee
- By phone: (209) 468-8700
- In writing:

  San Joaquin County Behavioral Health Services
  1212 N. California Street
  Stockton, CA 95202