Member Educational Resources – Protecting Your Health Information Online

As part of the CMS Interoperability and Patient Access Final Rule, Stanislaus County Behavioral Health and Recovery Services (BHRS) is committed to empowering members with access to their health information while ensuring they understand how to protect their privacy and security.

How to Protect the Privacy and Security of Your Health Information

When accessing your health information through third-party applications (apps), it's important to take steps to protect your privacy:

- **Use secure passwords**: Create strong passwords and never share them with others.
- **Enable multi-factor authentication (MFA)** when available.
- **Be cautious when downloading apps**: Only use trusted apps from reputable sources.
- **Review app permissions regularly** to ensure they only access necessary data.
- **Avoid using public Wi-Fi** when viewing personal health information.

Before using a health app, take the time to review its **privacy and security policies**. Make sure you understand how your data will be **used, stored, and shared**.

Understanding HIPAA and Non-HIPAA Covered Entities

It is important to know that not all health-related apps are protected by HIPAA (Health Insurance Portability and Accountability Act). The table below explains the difference:

Type of Organization/App	Likely HIPAA-Covered?	Oversight Agency
Your health plan or provider's patient portal	Yes	Office for Civil Rights (OCR)
Apps provided by third-party companies (not affiliated with your provider)	No	Federal Trade Commission (FTC)

HIPAA-covered entities (like your doctor or health plan) are legally required to protect your health information. **Non-HIPAA apps** may not have the same legal obligations and may share your data for **marketing or other purposes**.

Understanding 42 CFR Part 2 – Additional Protections for Substance Use Disorder Records

If you are receiving services for a **substance use disorder (SUD)**, your health information may also be protected under **42 CFR Part 2**—a federal regulation that provides **extra confidentiality safeguards** beyond HIPAA.

Key points about Part 2:

- **Applies to any federally assisted program** that provides SUD diagnosis, treatment, or referral to treatment.
- Requires **written patient consent** before disclosing information—even for treatment, payment, or health care operations.
- Violations of Part 2 can result in **legal consequences** for unauthorized disclosures.

Not all third-party health apps understand or follow Part 2 restrictions. Be cautious when sharing SUD-related health information through apps, and ensure you **fully understand how your information may be used or shared**.

Learn more: 42 CFR Part 2 on eCFR.gov

How to File a Complaint

If you believe an app has misused your personal health information or failed to protect your privacy:

- **For general health data issues:**
  File a complaint with the **Federal Trade Commission (FTC):**
  Visit www.ftc.gov/complaint
  Or call 1-877-FTC-HELP (1-877-382-4357)
- **For HIPAA-related violations:**
  File a complaint with the **U.S. Department of Health & Human Services – Office for Civil Rights (OCR):**
  Visit www.hhs.gov/ocr/privacy/hipaa/complaints

- **For 42 CFR Part 2 violations:**
  Contact your provider or program administrator to report a potential breach of confidentiality. Additional help may be available through legal aid or patient advocacy organizations.