Member Educational Resources

HIPAA (Health Insurance Portability and Accountability Act of 1996). This is a protection of your medical information. It is a federal law to make sure your doctors, nurses, and hospitals keep your personal health details private and safe. HIPAA shields your protected health information (PHI). PHI is any of the information in your medical record that can identify you. PHI can include, but is not limited to, your name, date of birth, social security number, diagnosis, etc.

Protecting Your Health Information – Understand the Security and Privacy Practices of Any Health Application You Trust Your Medical Records With:

- Review HIPAA Coverage
  - Read the application's privacy and terms of use, if your application is not associated with a HIPAA covered entity your data might not be protected.
- DATA Sharing Policies
  - Read the application's data policies to know if your data is sold or shared to a third party for advertising or marking purposes.
- Technical Safeguards
  - Make sure the application uses encryption. Encryption is a tool designed to make your data unreadable to people who are not allowed to your data. Make sure the application has a two-factor authentication. A two-factor authentication is a security process that requires two forms of identification to get to your data.
- DATA Control
  - Make sure you can delete or take back your consent to share data.

Some General Examples of Who is a HIPAA Covered Individuals and Organizations

- Healthcare Providers (The People Who Treat You)
  - Doctors
  - Dentists
  - Hospitals
  - Mental Health/Substance Use Facilities
  - Pharmacies
  - Therapists/Counselors
- Health Plans (People Who Pay)
  - Health Insurance Companies
  - Medicare and Medicaid
  - School Health Plans
- Healthcare Clearinghouses (The Data Processors)
  - These are companies that take the information from a doctor, for example, and put it in a format to send to insurance companies. This is how the doctor gets paid.

Some Examples of Who are NOT a HIPAA Covered Individual or Organizations

- Schools
  - Public schools use different laws to protect your records.
- Employers
  - A business that asks for medical records for employment-based reasons are not covered HIPAA entities
- Life Insurances Companies
  - Life insurance companies do not provide healthcare.
- Gyms and Fitness Applications
  - Applications used to track personal fitness are not linked to a HIPAA covered entity such as a healthcare provider.

Benefits of Payer-to-Payer and Provider Access API Exchange

- A Payer-to-Payer and Provider Access API exchange is a way to share your medical information in real time between plans and providers. Quick access can lead to:
  - Better care coordination and continuity of care
    - If you move to a new health plan your medical information transfers to your new health plan.
  - Faster authorization of services
    - Real time access to your medical information helps health plans find what they need to approve your medical care.
  - Greater customer service and medical care
    - Real time access to your records can close gaps in treatment. Providers can also provide improved case management to the services needed.
  - More accurate data
    - The use of old ways to record and transfer data that could create errors can be replaced.

Opt-In and Opt-Out Rights to Payer-to-Payer and Provider Access API Exchange with Instructions

- You have the right to opt-in and opt-out of this type of data exchange. It is not required for you to use this service. You will not automatically be enrolled.
- You can opt-in or opt-out of this service with Partnership by completing the form found at this link.

- Once the form is complete it can be returned by fax or mail:
  - (707)863-4415
  - Partnership Healthplan of California
    Attn: Members Services
    4665 Business Center Drive
    Fairfield, CA 94534

Where to file complaints:

- **Office of Civil Rights (OCR)**: Part of the U.S. Department of Health and Human Services (HHS), OCR enforces HIPAA privacy and security rules for covered entities. It investigates complaints and conducts audits to ensure compliance.
  - To file a complaint online with OCR using the OCR complaint portal visit https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf. To learn more about filling a complaint with OCR under HIPAA, visit: https://www.hhs.gov/hipaa/filing-a-complaint/index.html.
  - If you have any questions or need help filing a civil rights, conscience or religious freedom, or health information privacy complaint, you may email OCR at OCRMail@hhs.gov or call the U.S. Department of Health and Human Services, Office for Civil Rights toll-free at 1-800-368-1019, TDD: 1-800-537-7697.
  - Mail: Send a written complaint to the appropriate regional OCR office.
- **Federal Trade Commission (FTC)**: The FTC plays a role in enforcing privacy and security standards for non-HIPAA-covered entities, such as mobile health apps and health-related websites. It promotes consumer protection and addresses deceptive or unfair practices.
  - Visit the FTC website and use the Complaint Assistant tool: https://reportfraud.ftc.gov/.
  - If you are unable to use the online tool, you can call the FTC's Consumer Resource Center at 1-877-382-4357.