A Shared Responsibility: Protecting Member and Patient Information

Partnership HealthPlan of California and its contracted providers share a responsibility to protect member and patient information, in oral, written and electronic formats. As a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), you have an obligation and responsibility to protect your patient's and our member's Protected Health Information (PHI). If there is a situation where an individual or organization has suspicion or reason to believe PHI may have been lost, sent in an unencrypted format, or otherwise provided to an individual or organization that does not have a right to review or receive the PHI, this is considered a breach and must be reported to Partnership.

Below are questions and answers to help you understand HIPAA and your responsibilities as a Partnership provider:

What is HIPAA?
HIPAA is a Federal law that protects PHI. PHI includes any information that can be used to identify a member or patient.

What is a HIPAA breach?
A breach, also known as a privacy incident, may be accidental or intentional. The release of PHI in a privacy incident may be in a variety of formats: oral, written, and electronic.
The list below includes examples of some potential privacy incidents that should always be reported to Partnership:

1. **PHI sent to the wrong individual or organization**
   An example of this is sending a fax to the wrong number or mailing PHI to the wrong address/individual.
2. **Unsecure email with PHI**
   An example of this may include PHI that is accessed electronically or sent to an unauthorized individual by email, and the PHI is not encrypted.
3. **Theft**
   An example of this may include PHI that is stolen due to the theft of an unencrypted or unprotected laptop or desktop; theft of hard drives or other media with PHI that is not encrypted, or theft of paper PHI.
4. **Security data breaches**
   An example of this may include PHI that is stolen due to planned breaches through malware or viruses that corrupt data resources, password, and computer system attacks.

A Shared Responsibility: Protecting Member and Patient Information

What kind of information is protected?

PHI is personal information that can identify a member/patient, including but not limited to:

- Names
- Dates of birth
- Addresses
- Social Security Numbers (SSN)
- Client Identification Numbers (CIN)
- Bank account numbers

How soon after a loss or theft must the report be made to Partnership?

Reports should be filed with Partnership immediately (within 24 hours) or as soon as the incident is identified.

If I already notified another agency, do I still have to notify Partnership?

Yes. We are required to notify the proper regulatory agency, regardless of any reports your office may have made to any other agency.

How soon after a loss or theft must the report be made to Partnership?

Reports should be filed with Partnership immediately (within 24 hours) or as soon as the incident is identified.

How do I report a HIPAA breach to Partnership?

Providers should contact Partnership as soon as your office is aware a potential privacy breach.

Report discovery of incident within 24 hours by:

- **Fax:** (707) 833-4363
- **Email:** RAC_Reporting@partnershiphp.org
- **Call our Compliance Hotline:** (800) 601-2146

*For those who prefer to may remain **anonymous** please call the Compliance Hotline.*

Reminder to all Providers:

This serves as a formal reminder to all providers that it is a requirement to obtain approval from the Department of Health Care Services (DHCS) before sending any member notices or letters.

Note: If you have questions about this information, send them to Partnership's Provider Relations Department.

Contact our Provider Relations Department:

- **Email**: eSystemsSupport@Partnershiphp.org
- **Office number:** (707) 863-4100
- **Office hours:** Monday-Friday from 8 a.m.-5 p.m.