A Shared Responsibility
Protecting Member/Patient Information

Partnership HealthPlan of California (PHC) and its' contracted providers share a responsibility to protect member/patient information, in oral, written and electronic formats. Any time a PHC member's information is lost in a breach, you must notify PHC so that a report can be filed with the proper regulatory agency regarding the details of the lost information. The following are some questions and answers to help you understand HIPAA and your responsibilities as a PHC provider.

Note: If you have questions about this information, send them to the PHC Provider Relations Department.

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPPA) is a Federal law that protects Protected Health Information (PHI). PHI includes any information that can be used to identify a member or patient.

What is a HIPAA Breach?

A HIPAA Breach occurs whenever member or patient information is lost. This can happen by accident or theft.

What kind of information is protected?

PHI, includes any 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

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

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 PHC?

Reports should be filed with PHC immediately; as soon as the breach is identified.

How do I report a HIPAA breach to PHC?

Providers should contact the PHC Privacy Officer as soon as they are aware that a breach occurred. You can contact the PHC Privacy Officer by phone at **707-420-7625**, or by mail to 4665 Business Center Drive, Fairfield CA, 94534.

Partners in Fighting Fraud
Doing Your Part as a Provider

Fraud: An intentional act of deception, misrepresentation, or concealment in order to gain something of value.

Waste: Over-utilization of services (not caused by criminally negligent actions) and the misuse of resources.

Abuse: Excessive or improper use of services or actions that is inconsistent with acceptable business or medical practices. This refers to incidents that, although not fraudulent, they may directly or indirectly cause financial loss.

Examples Include:

- Charging excessive costs for services or supplies
- Providing medically unnecessary services
- Billing for items or services that would not be paid for by Medicare
- Billing for services that were not provided
- Billing for services at a higher rate than is actually justified
- Misrepresenting services resulting in unnecessary costs to the Medicare program, improper payments to providers or overpayments

Fraud related losses in health care programs amounts to billions of dollars each year. All programs, such as Medi-Cal and Medicare are vulnerable to fraud. Partnership Health Plan of California (PHC) asks that their providers and employees join the fight against fraud by referring suspicious and fraudulent activity to the resources that follow. The California Department of Health Care Services (DHCS), the California of Managed Health Care (DMHC), and the Centers for Medicare and Medicaid Services (CMS) require that PHC maintains a robust anti-fraud plan and share it with its' providers, members and employees. You can find updated policies and procedures, provider and practitioner manuals and the PHC Formulary at www.partnershiphp.org

The PHC Anonymous Fraud Hotline - Call 800-601-2146

Members, providers and employees can call the fraud hotline 24 hours a day, 7 days a week to report suspicious and fraudulent activity anonymously. Reports are forwarded to PHC for review.

Medi-Cal Fraud Issues - Call 800-822-6222

Providers and members should call the Bureau of Medi-Cal Fraud and Elder Abuse. Providers and members can also call PHC to report suspicious and fraudulent activity, however members and providers will also be referred to the State for complete reporting.

Medicare Fraud Issues

Medicare Members have several resources for reporting fraud, other than PHC. Members can call the Health Insurance Counseling and Advocacy Program (HICAP) to speak to fraud specialists before speaking to CMS or the Office of the inspector General (OIG). Providers can call CMS, PHC, or HICAP on behalf of a member.

CMS Call: **800-633-4221** **HICAP** Call: **800-434-0222** **OIG** Call: **800-447-8477**

For Providers: Call the PHC Provider Relations Department 1-707-863-4100

For Members: Call the PHC Member Services Department 1-800-863-4155

Protected Health Information
Sending Secure Email

Partnership HealthPlan of California (PHC) Cultural and Linguistic Committee has coordinated a toolkit to educate providers about documenting patient language needs in medical charts, accessing interpreter services and referring patients to culturally and linguistically appropriate community service programs.

The Health Insurance Portability and Accountability Act (HIPAA) act was designed to protect patients protected health information (PHI) from being accessible to the general public. As more clinicians are transmitting patient records and personal information to other parties electronically, it is imperative that we all ensure that patient information is secure.

PHI includes any data 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

If any information in an email can be used to identify a member, the email must be sent using secure methods. Sending secure email requires an extra step to ensure the email is properly protected.

Secure Email Best Practices

- If you are not sure whether the information in the email can be considered PHI, always err on the side of caution. If you think, a piece of information can be used to identify a member, use secure email to send it electronically.
- Never put PHI in the subject line of emails. Secure emails only secure the body of the email, but not the subject line contents. Use generic descriptions of your email for the subject line and keep any PHI or sensitive information in the body of the email.
- Verify email addresses before sending an email to ensure it is sent to the correct person. The person emailed can only open the secure email that is sent. If the recipient is the wrong person, that person can see the content of the email. This can result in a HIPAA breach.
- Carefully review the email subject line and content, then confirm all recipients in the To, CC and BCC fields, before sending the email.

Following these practices ensures your patient and business information is kept confidential and protected. Addressing email security should be part of every company's business plan. Your organization's IT Department can provide you with information on sending secure email.