



Subject:	<b>Security Incident Procedures</b>	Policy No:	AS110
Signature		Original Issue:	4/12/05
SEC Approval:	Marilee McGuire	Date:	7/13/05
Prepared By:	Jeff Cains	Effective Date:	7/22/05

**Purpose:**

The purpose is to implement policy and procedures to address security incidents at Community Health Plan (CHP). CHP will create processes for the identification, reporting, and timely response to real or potential violations of the security or a material breach of any part of CHP's security policy.

**Scope:**

This policy applies to CHP in its entirety, all workforce members, including consultants, contractors, business associates and vendors. In addition, some third parties such as contractors or vendors will be required to abide by parts of this policy if required by CHP in a Business Associate Agreement (BAA) or under applicable law.

**Policy:**

CHP will maintain procedures for identifying security incidents. Generally, a security incident includes network, host activity, and misuse of data that may risk the security of electronic PHI (ePHI). A security incident may also include a breach of security policy or any activity that could potentially put sensitive and/or confidential information at risk of unauthorized access or modification.

Incidents will be classified as "serious" or "non-serious."

**Serious incidents** generally have the following characteristics:

- It is determined that there was malicious intent and the attack was specifically directed specifically at CHP
- Or**
- It is determined that sensitive information, especially ePHI, may have been accessed or damaged in an unauthorized manner

**Non-serious incidents** generally have the following characteristics:

- It is determined that there was no malicious intent directed toward CHP
- And**
- It is determined that no sensitive information, especially electronic protected health information (ePHI), was used, disclosed, or damaged in an unauthorized manner

Consultants, contractors, business associates and vendors of CHP must report any security incident to the Security Officer that they become aware of or suspect.

CHP will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature.

Incidents characterized as serious by the Security Officer will be responded to immediately and reported to the Compliance Officer and appropriate upper-level management. The Security

Officer, in consultation with the Compliance Officer, will determine if an incident is appropriate to report to outside entities based on business and legal considerations.

CHP will attempt to mitigate any harmful effects, when possible, where a security incident affects customer or member information.

CHP will develop security policies to identify core activities in the area of Response and Reporting implementation specification of the HIPAA Security Rule. These policies will include incident reporting procedures to outside entities as required by law or as determined appropriate, based on business and legal considerations.

A copy of this Policy will be retained for a minimum period of six (6) years from the date it was created or, if revised, for a minimum period of six (6) years from the date it was last in effect.

**Responsibilities:**

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Staying aware of and identifying potential security incidents
- Reporting any suspected security incident to the Security Officer
- Assisting the Security Officer in ending the security breach and mitigating its harmful effects, if possible

The Security Officer is responsible for:

- Maintaining all security incident-related policies and procedures
- Characterizing all reported security incidents as “serious” or “non-serious” as per the guidelines outlined above. The Security Officer may take into account the professional expertise and experiences of department management
- Maintaining procedures for responding to security incidents
- Documenting all reported security incidents and their outcome
- Leading compliance activities that bring CHP into compliance with the HIPAA Security Rule implementation specifications of Response and Reporting.

The Security Officer and other members of management are jointly responsible for:

- Mitigating, to the extent possible, any harmful effects of security incidents
- Deciding when it is appropriate to contact law enforcement officials about a security incident that has been characterized as serious

The Compliance Officer or designee is responsible for:

- Tracking PHI disclosure information per the Accounting of Disclosures of PHI policy, as appropriate.
- Conducting notifications of affected parties for reportable breaches as described under “Notice of Security Breaches”

**Compliance:**

Failure to comply with this or any other security policy will result in disciplinary actions as described in the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Security Incident Procedures is a standard (164.308 (a)(6)) defined in the Administrative Safeguards category of the HIPAA Security Rule.

**Procedure(s):**

Procedures related to the Security Incident Response Policy include:

- Security Incident Response Procedure
- Security Incident Documentation Procedure

## **Security Incident Response Procedures**

As end users, management or Information Technology Infrastructure team members, consultants, contractors, business associates and vendors may become aware of a Security Incident. The procedures for responding to Security Incidents are outlined below:

### End users

End users include all individuals employed by CHP in anyway such as payroll workforce members, contractors or vendors. End users may become aware of Security Incidents by:

- Witnessing or being made aware of "potential" unauthorized disclosure of PHI or ePHI
- Witnessing or being made aware of internal or external hacker activities
- Computer alerts from virus scanning or spyware scanning software

When end users becomes aware of a Security Incident they should immediately take whatever steps appropriate to prevent disclosure of PHI or ePHI (i.e. removing paper documents from public areas that might contain PHI, locking computers displaying ePHI, etc) and immediately report the incident to an available manager. In addition, if the incident involves a potential threat to ePHI from hacker activities or computer viruses, the end-user should immediately report the incident it to the Help Desk.

### Managers

Managers may become aware of Security Incidents by:

- Being informed by end users of a potential security incident
- Witnessing or being made aware of "potential" unauthorized disclosure of PHI or ePHI
- Witnessing or being made aware of internal or external hacker activities, including reports from end users
- Computer alerts from virus scanning or spyware scanning software

When managers become aware of a Security Incident, they should immediately take whatever steps appropriate to prevent disclosure of PHI or ePHI (i.e. removing paper documents from public areas that might contain PHI, locking computers displaying ePHI, etc) and immediately report the incident to the Security Officer. In addition, if the incident involves a potential threat to ePHI from hacker activities or computer viruses, the manager should immediately report the incident it to the Help Desk, unless an end-user has already done so.

### Information Technology Infrastructure Team Members

Information Technology Infrastructure (ITI) team members may become aware of Security Incidents by:

- Being informed by end users or managers of a potential security incident
- Witnessing or being made aware of "potential" unauthorized disclosure of PHI or ePHI
- Witnessing or being made aware of internal or external hacker activities via the Intrusion Detection Program; security, application, and firewall logs; and reports from end users or managers
- Computer alerts from virus scanning or spyware scanning software and reports from end users or managers

When ITI team members becomes aware of a Security Incident they should immediately take whatever steps appropriate to prevent disclosure of PHI or ePHI (i.e. removing paper documents from public areas that might contain PHI, locking computers displaying ePHI, etc) and immediately report the incident to the Security Officer. In addition, if the incident involves a potential threat to ePHI from hacker activities or computer viruses the ITI team member will take whatever steps necessary to remediate the threat. These steps will be identified and documented by IT.

### Notice of Security Breaches

CHP shall disclose any breach of the security of the system containing unencrypted personal information following discovery or notification of the breach in the security of the data to any Washington State resident whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. A reportable breach does not include a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

- The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If this is the case, the notification shall be made after the law enforcement agency determines that it will not compromise the investigation.
- For the purposes of this policy, a “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by CHP.
- For the purposes of this policy, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - Social security number
  - Driver’s license number or Washington identification card number; or
  - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
- “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- Notice may be provided by one of the following methods:
  - Written notice;
  - Electronic notice, if provided consistent with the electronic records and signatures provisions of 15 U.S.C. Sec. 7001; or
  - Substitute notice, if the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or CHP does not have sufficient contact information. Substitute notice shall consist of the following:
    - E-mail notice when CHP has an e-mail address for the subject persons;
    - Conspicuous posting of the notice on the CHP website; and
    - Notification to major statewide media.

### **Form(s):**

Security Incident Documentation Log

### **Definition(s):**

Definitions for all policies are included in the glossary section of the Appendix.

**References:**

HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>, February 20, 2003.

- Getting Started with HIPAA, Uday O. Ali Pabrai, Premier Press, April 2003.
- CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS, February 2002.
- International Standards Organization (ISO/IEC 17799:2000(E))
- SSB 6043 Personal Information – Notice of Security Breaches

**Contact:**

See Master Contacts List

Revision History		
Revision Date	Revision	Revision Made By
7/11/05	Addition of section "Notice of Security Breaches" and applicable language in compliance with SSB 6043 requirements	Carrie Hardie
7/11/05	Removal of Contacts and consolidation in Master Contact List	Carrie Hardie
3/22/06	Changed all references from "Community Health Plan of Washington" to "Community Health Plan" and "CHPW" to "CHP"	Carrie Hardie