



COMMUNITY HEALTH PLAN
of Washington

Committed to your health.

Subject:	Security Policy	Policy No.: PS106
Signature		Original Issue: 4/12/05
SEC Approval:	Marilee McGuire	Date: 4/11/05
Prepared By:	Carrie Hardie	Effective Date: 4/20/05

Purpose:

The purpose of this policy is to implement policies and procedures consistent with HIPAA Security requirements, including those specific requirements regarding physical safeguards (45 CFR § 164.306). Physical safeguards are the physical measures, policies, and procedures intended to protect Community Health Plan (CHP) electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. There are four standards for physical safeguards, including Facility Access Controls, Work Station Use, Workstation Security, and Device and Media Controls.

This policy addresses CHP's Facility Access Controls through the implementation of policies and procedures to limit physical access to Community Health Plan's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Reasonable building security for persons and property at CHP will be accomplished through:

- Limited card access authorization and the control of keys issued
- Ensuring appropriate access to work areas by CHP workforce members in CHP offices.

In addition, guidance regarding procedures for Safeguarding Confidential Information has been provided as a quick reference for workforce members. Workforce members must review the full policy and procedure referenced for complete information.

The specific physical facilities include offices in the 720 Olive Building and any other areas where CHP manages information technology facilities or network wiring rooms.

Scope:

This policy applies to Community Health Plan in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit electronic protected health information (ePHI).

Policy:

CHP will launch activities to ensure compliance with the Facility Access Control standard and its associated implementation specifications of Contingency Plan, facility security plan, access control and validation procedures, and maintenance records.

CHP will safeguard the facility and equipment from unauthorized physical access, tampering and theft.

CHP will continually assess potential risks and vulnerabilities to ePHI and develop, implement and maintain appropriate safeguards to ensure compliance with the requirements of the HIPAA Security Rule.

All repairs and modifications to the physical components of the facility shall be documented and maintained by the Security Officer.

All repairs and maintenance, including installation, of hardware and software will be documented and maintained by the Security Officer.

The Facility Security Plan shall be reviewed and updated at least once every year.

Maintenance of all hardware and software will be reviewed on an annual basis.

Tests on the security attributes of all hardware and software will be conducted on an annual basis.

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:

The Security Officer is responsible for ensuring the implementation of the requirements of the Facility Access Control standard and its associated implementation specifications of Contingency Plan, facility security plan, access control and validation procedures, and maintenance records.

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 the HIPAA Privacy and Security Rules.

Procedure(s):

Facility Access Control Guidelines

Facility Access Controls is a standard (164.310 (a)(1)) defined in the Physical Safeguards category of the HIPAA Security Rule. Each CHP employee is responsible for the security of his or her individual office and general work area (where possible in the open cubicle environment). Additionally, where applicable, workforce members are also responsible for security of the entire building and supplies. The following guidelines will assist workforce members in this endeavor:

Office Hours

CHP's business hours are Monday through Friday, 8:00 A.M. to 5:00 P.M. (except for official company holidays).

ID Badges and Access Cards

All CHP workforce members are required to wear an employee ID badge visibly displayed at all times while on CHP premises. Facilities and Human Resources will ensure that a photo ID badge and access card are issued to new workforce members within 3 days of hire. New employees must wear their "temporary" badge until the photo ID badge is issued to them. All CHP workforce members must use their access cards to gain entry to secure areas of the facility.

All individuals in CHP buildings and facilities must have an identification badge visibly displayed on their person. Workforce members have a duty to question any unescorted visitors or individuals they do not recognize and immediately report any unauthorized personnel to the Security Officer and Facilities.

CHP has a "one card, one entry" policy. This means that each employee must pass his or her access card across a card reader at each secured entry point, even if another employee has already entered the area ahead of him or her.

Workforce members must ensure that secure doors are locked when entering and leaving the building after normal business hours. Workforce members are not allowed to lend their building or office keys, or access card, to anyone.

Lost ID badges and access cards must be reported to the Reception Desk immediately. Workforce members may check out a "loaner" badge each day for a maximum of three consecutive days; after the third day, the badge or card is considered lost and a card replacement fee of \$20 will be assessed. The "loaner" log will be monitored and the results will be shared with CHP management, who will be responsible for appropriately disciplining policy violators in accordance with the Sanction Policy.

Building Management Staff

Building management staff shall coordinate all activities within CHP offices with Facilities and the Reception Desk. If it is not an emergency situation, advance notice will be provided to CHP workforce members that building staff will be in CHP offices performing maintenance duties. Building management workforce members must be clearly identified by a building-issued identification badge at all time while in CHP offices.

If a vendor who is not a building management employee is authorized to perform maintenance work within CHP offices, he or she must check in with the Reception Desk and follow all visitor procedures, except for the requirement of an employee escort. Facilities will notify CHP workforce members of the scheduled time and location of the work.

Maintenance Records

Facilities is responsible for establishing a policy and procedure for maintaining a record of all maintenance to physical components as required under 45 CFR §164.310. IT is responsible for establishing a policy and procedure for maintaining a record of all maintenance to information systems and related hardware, pursuant to 45 CFR §164.310. See Maintenance Records policy for more detail.

Maintenance records will be maintained by the appropriate department for a period of no less than six (6) years.

Visitors

All visitors (defined as any individual who is not a member of the CHP workforce, including vendors, delivery personnel, and meeting guests) are required to report to a Reception Zone (defined below), where they are required to sign in at the visitor log. The reception desk staff will issue a clearly marked "Visitor" badge to the visitor, which must be visibly displayed on the visitor's person at all times while on CHP's premises.

Visitors must be escorted by a CHP employee within reasonable limits (e.g., escort is not necessary for the restroom) when the visitor is within CHP controlled security areas. When the visitor departs CHP premises, the employee escort of the visitor must ensure that the visitor signs back out of the visitor log and returns the visitor badge to the reception desk.

The Reception Desk will maintain a list of vendors who do not require an escort while in CHP offices due to the nature of their work (e.g., coffee supplier, copier or fax machine technician). These vendors are still required to check in and out at the Reception Desk and wear a Visitor badge per the Visitor procedures, and will be required to sign Confidentiality and Non-Disclosure Agreements.

The Reception Desk will audit the visitor log on a weekly basis to ensure that all ID badges are accounted for and that all visitors have been properly signed out.

Visitors are not allowed access to the Server Room without prior authorization. Workforce members should contact IT for further guidance regarding Server Room access, including for visitors.

IT will establish procedures for controlling access software programs for testing and revision. All software vendors must execute a Business Associate Agreement before being granted access to CHP work areas or systems. Software vendor workforce members must comply with the visitor procedures described in this policy, including being escorted by a CHP IT employee while on the premises. IT will grant the vendor only the level of access appropriate, based on the vendor's job function and business need, to perform testing, maintenance or revision to information technology resources (computer networks, telephone lines, data transmission lines, etc).

The Security Officer or the CEO may issue special permission for individuals to be in the building without the escort of a staff member or display of a visitor badge. Such cases will be previously announced to CHP staff and include large groups of people, i.e. training classes, where attendees are not required to have an escort.

Contingency Plan

Facilities and IT are responsible for establishing, evaluating, and updating CHP's Contingency Plan policy and procedures, which will include procedures for a Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan. See the Contingency Plan Policy for more detail.

Workstation Use and Security

In order to safeguard sensitive information, such as PHI and other confidential data, workforce members may need to restrict others from entering their cubicle when such information is displayed, turn off their computer monitor, minimize the window they are working on, and/or turn PHI face-down on their desks.

Access to PHI is restricted to workforce members who have a "need to know" the information and subject to the Disclosing and Seeking Only the Minimum Amount of PHI Necessary Policy. Workforce members are prohibited from attempting unauthorized and non work-related access. IT will establish access permissions for workforce members to systems and software based on job-related function, and need to access PHI will be detailed in the job description.

Workforce members must ensure that sensitive material in their possession is locked up when not in use, and prior to departing their office for the day. Laptops and other electronic computing devices must also be secured at the end of the day (e.g., locked in a desk drawer). All workforce members must manually "lock" PCs (by hitting Ctrl-Alt-Delete and selecting "Lock Computer") each time they leave a PC where they have logged in to prevent unauthorized access.

Where possible, workstations will be configured for monitors to face away from aisles or other areas where passersby could view the information on the PC. If not feasible, workforce members will employ other reasonable methods to obscure confidential information on monitors, such as special screens, as instructed by Facilities.

Workstations must be labeled to identify function and location and to assist with compliance with access control procedures. In addition, all workstations must be operated in a manner that ensures the display of an IT-designated warning banner prior to gaining operating system access. In addition, all workforce members must ensure the proper log off of workstations at the end of the business day.

CHP shall ensure sufficient illumination in and around facilities to allow the detection and observation of persons approaching the building and to discourage criminal activity. CHP Departments may need to work with Facilities to arrange for additional building services, i.e. improved lighting.

Device and Media Controls

Disposal of Confidential Information

Confidential information, including paper PHI, must be placed in the secure shred bins for disposal. Workforce members must not place any confidential information in trash receptacles.

Electronic confidential information, including PHI, must be disposed of in accordance with IT policies and procedures. This includes data contained on CDs, DVDs, USB drives, tapes and diskettes (this list is not exhaustive). Refer to the Disposal Policy for more information.

Media Re-Use

CHP must ensure that prior to reusing any media, such as DVDs, external hard disk drives, and CDs, it is securely overwritten and that this action is verified and documented. Workforce members that have media containing PHI that they would like to reuse must first contact IT for guidance about appropriate methods to overwrite the data. Refer to the Media Re-Use Policy for more information.

Accountability

CHP will ensure that a record is maintained to identify movements of ePHI-related hardware and devices. The movement of hardware, electronic media and devices includes the receipt, removal, storage and/or disposal of ePHI systems. Such information will also include the identity of responsible persons associated with the movement.

IT is responsible for maintaining the record of movement of hardware, electronic media and devices. See Accountability Policy for more information.

Data Backup and Storage

CHP will ensure the secure receipt, transport, and removal of:

- Computer Equipment
- Software
- Electronic media, such as diskettes, tapes, CD/R/RWs, USB storage devices, DVDs, zip disks, Jazz drives, removable hard drives, internal hard drives and external hard drives

In addition, the IT Department will document the following:

- Who has control of the hardware/software/or electronic media at all times
- Accountability, the ability to ensure that the actions of an entity can be traced back to that specific entity
- Data backup
- Data storage
- Disposal
- Retrieval
- Archiving and Retrieval testing

See Data Backup and Storage Policy for more information.

Safeguarding Confidential Information

The following information is intended to provide a brief summary of the information contained in the full policies as referenced below. Workforce members should not rely solely on this information. Furthermore, workforce members are responsible for complying with the policies and procedures as described more fully in the following policy and procedures:

- Electronic Communications Policy
- E-mail Security & Acceptable Use Policy
- PHI Transmitted by Fax Policy
- Disposal Policy

Email

All email messages containing confidential information that are being transmitted to a recipient outside of the CHP network (to any recipient whose email address does not end in "@chpw.org") must first be encrypted using the method described in the Encryption Policy. Acceptable encryption methods include PGP encryption and WinZip 9.0 encryption. Refer to the E-mail Security & Acceptable Use Policy for additional information.

All workforce members sending email should double-check the "To" line to ensure that only the intended recipients are listed.

Transmission of email containing PHI is restricted to only those purposes permitted under the Privacy Rule, and must be limited to the minimum necessary information, as appropriate. If workforce members are unsure if the PHI is being disclosed for a permitted purpose, they should first check with their manager or the Compliance Officer for guidance.

Faxes

Faxes containing PHI must comply with the requirements of the PHI Transmitted by Fax Policy. Requirements include that faxing PHI be limited to urgent situations where mail or other delivery is not feasible, and not faxing sensitive health information (including information about mental illness, substance abuse, STDs, or reproductive health).

Misdirected faxes must be reported immediately to the Compliance Officer.

Passwords

There are specific requirements for management of passwords, as described in the E-mail Security & Acceptable Use Policy (see the policy for complete details).

Passwords for *all* systems are subject to the following rules:

- Passwords must not be spoken, written, e-mailed, hinted at, shared, or in any way known to **anyone** other than the user to whom the password has been issued. No exceptions are allowed for supervisors or assistants.
- Passwords must not be shared in order to "cover" for someone out of the office. Contact the Help Desk to set up a temporary account if there are resources you need to access.
- Passwords must not be your name, address, date of birth, username, nickname, or any term that could easily be guessed by someone who is familiar with you.
- Passwords must not be displayed or concealed on your workspace.

Individuals may attempt to gain unauthorized access to CHP computing resources and systems by employing social engineering techniques on workforce members, such as posing as a "system administrator" and asking for an employee's password. **IT will not ask workforce members for their password, as IT staff already have access to employee files due to system administrator privileges.** Workforce members must be wary of any person asking for password or system information, and should contact IT for verification of the requestor's identity prior to disclosing any information to him/her. The rule is: "when in doubt, ask IT".

CHP Management Responsibilities

- Safeguarding sensitive and/or confidential information under their control including printed information, PHI, PC desktop information, and electronic information.
- Protecting assets by locking up what can be locked up in offices, file drawers, and overhead drawers, and contacting the Security Officer and Facilities when assets are found missing or misused.
- Providing staff education about this policy, monitoring staff adherence to the security policies and procedures, and addressing non-compliance with staff as provided for in the CHP Sanction Policy.

Form(s):

None

Definition(s):

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

Policy Reference:

- Disposal Policy
- PHI Transmitted by Fax Policy
- Maintenance Records Policy
- Contingency Plan Policy
- Sanction Policy
- Disclosing and Seeking Only the Minimum Amount of PHI Necessary Policy
- Data Backup and Storage Policy
- Media Re-Use Policy
- Accountability Policy

References:

- HIPAA Final Privacy Rule, 45 CFR Parts 160 through 164
- 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))

Contact:

See Master Contacts List

Revision History		
Revision Date	Revision	Revision Made By
10/24/05	Removal of Contacts and consolidation in Master Contact List	Carrie Hardie
3/22/06	Changed references to "Encryption	Carrie Hardie

	Policy” and “Password Policy” to “E-mail Security & Acceptable Use Policy”	
3/22/06	Changed all references from “Community Health Plan of Washington” to “Community Health Plan” and “CHPW” to “CHP”	Carrie Hardie
9/8/06	<p>Revisions are as follows:</p> <ul style="list-style-type: none"> • Page 1: corrected citation in first paragraph • Page 2: added “visibly displayed” to first sentence under “ID Badges and Access Cards”. Also added “new employees must wear their ‘temporary’ badge until the photo ID badge is issued to them.” Reference to “Office Services Supervisor” changed to “Facilities”. • Page 3: replacement card fee changed to \$20 • Page 4: reference to “CFO” changed to “CEO”. Also clarified procedure for manually locking computer under third paragraph of “Workstation Use and Security”. Removed requirement to shut down PCs at end of day. Also removed reference to security zones. • Page 7: reference to “Office Services Supervisor” changed to “Facilities” 	Carrie Hardie