COMMUNITY HEALTH PLAN of Washington

Committed to your health.

Subject:	**Access Authorization and Termination Policy**	Policy No.: AS113
Signature		Original Issue: 8/12/05
SEC Approval:	Marilee McGuire	Date: 8/8/05
Prepared By:	Carrie Hardie	Effective Date: 8/12/05

Purpose:
The purpose of this policy is to implement procedures for setting up, modifying, and terminating access to facilities and systems, including electronic Protected Health Information (ePHI), when the employment of a workforce member begins, changes, or ends.

Scope:
This policy applies to Community Health Plan (CHP) in its entirety, including all workforce members.

Policy:
CHP recognizes the importance of ensuring appropriate workforce access to systems and facilities, and particularly the importance of protecting our assets from unauthorized personnel.

In compliance with applicable laws and regulations, including HIPAA, CHP will establish procedures for initial access set up for new workforce members, modification of access for job function changes, and termination of access following employment separation.

The workforce member's supervisor is responsible for promptly notifying IT, HR, and other affected departments of new workforce members, including temporary employees, and, in coordination with Facilities, ensuring that physical access permissions are set up appropriately. IT is responsible for setting appropriate system access permissions based on job function.

After appropriate approvals are obtained, the workforce member's supervisor is responsible for promptly notifying IT and other affected departments of a job function change that may require adjustment to systems access permissions, in order that IT may modify access for that workforce member accordingly.

The workforce member's supervisor is responsible for promptly notifying IT, HR and other affected departments of the voluntary separation of workforce members to include, but not limited to employees and temporary workers, in order that Facilities may immediately terminate physical access, and IT may immediately terminate system access for that workforce member.

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.

Procedure:

<u>New workforce (including temporary staff and contractors)</u>

1. The hiring supervisor will send a completed MAC form (located in the Outlook Public Folders, under Outlook Templates) to the MAC Form Recipients distribution list no later than five business days prior to the new workforce member's start date. Any exceptions

to the deadline must be explained in the "Comments" section of the MAC form. Short notice may delay setup by IT for the new hire.

2. HR will ensure that all required forms are completed and returned by the new workforce member, including the Sanction Screening and Confidentiality forms.
3. Facilities will issue a photo ID badge, access card, and any necessary keys to the new workforce member on his or her start date. Facilities is responsible for logging, tracking, and auditing records related to the ID badges, access cards, and keys, including ensuring that "loaner" and visitor badges and access cards (if appropriate) are returned and accounted for.

Terminated workforce

1. The workforce member's supervisor will send a completed MAC form to the MAC Form Recipients distribution list no later than three business days prior to the workforce member's termination date.
2. In the event of an involuntary termination, HR will timely notify IT and Facilities of the termination.
3. Once notified of a workforce member's termination, IT is responsible for ensuring that:
   - Password access is immediately revoked in the event of an involuntary separation, and scheduled to be revoked on the last day of employment for voluntary separations and at the end of temporary assignments for any workforce members.
   - Access to all systems and applications is revoked immediately in the event of involuntary terminations, and scheduled to be revoked on the last day of employment for voluntary separations and at the end of temporary assignments for any workforce members.
   - The workforce member is removed from any systems or applications that processed ePHI immediately in the event of involuntary terminations, and scheduled to be revoked on the last day of employment for voluntary separations and at the end of temporary assignments for any workforce member.
4. HR, Facilities, and the workforce member's supervisor must coordinate to ensure that:
   - Any keys and IDs provided to the workforce member during their employment are returned on the scheduled last day of employment, or immediately upon notice of involuntary separation.
   - In the event of an involuntary separation, the workforce member's supervisor and/or HR provides the workforce member limited and carefully supervised access to their desk or office.
5. HR will conduct an exit interview for employment separations and document any issues or concerns related to the workforce member as appropriate.

Change in Job Function

1. The workforce member's supervisor will send a completed MAC form to the MAC Form Recipients distribution list no later than three business days prior to the effective date of the workforce member's change in job function.
2. After appropriate approvals are obtained, the workforce member's supervisor is responsible for promptly notifying IT and other affected departments of a job function change that may require adjustment to systems access permissions, in order that IT may modify access for that workforce member accordingly.

Responsibilities:

The following staff are responsible for the duties identified in this policy as follows:

- The Security Officer is responsible for ensuring that all information systems-related activities identified in this Termination Procedure document are followed through and implemented.

- The workforce member's supervisor is responsible for the management duties identified in this policy.
- Human Resources is responsible for the HR functions identified in this policy.
- Information Technology is responsible for the IT functions identified in this policy.
- Facilities is responsible for the facilities-related functions identified in this policy.

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

Form(s):
MAC Form

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))

Contact:

See Master Contacts List

Revision History		
Revision Date	Revision	Revision Made By
3/22/06	Changed all references from "Community Health Plan of Washington" to "Community Health Plan" and "CHPW" to "CHP"	Carrie Hardie