COMMUNITY
HEALTH NETWORK
of Connecticut

POLICY AND PROCEDURES

SUBJECT: Privacy- Privacy and Security Audits

P&P #	DATE ISSUED	DATE REVIEWED	DATE REVISED
CMPL144	04/14/03		
REPLACES POLICY #	**DATE RETIRED**		

Date	**Compliance Officer**	**Date**	**Chief Executive Officer**
Date	**Manager, Technical Services**	**Date**	**Chief Information Officer**

PURPOSE:

Community Health Network Of Connecticut (CHNCT) is required by federal and state laws to protect the confidentiality and privacy of our member health information. It is of equal importance to treat employee personnel information and provider credentialing files in a confidential manner. The purpose of this policy is to provide guidance to employees on the privacy and security audits that will be conducted throughout CHNCT.

POLICY:

CHNCT will conduct routine privacy and security audits to assure compliance with various federal and state laws and internal policies regarding confidentiality. By conducting these audits, CHNCT hopes to promote the importance of confidentiality regarding member health information, employee personnel information and provider credentialing files. Those employees who do not pass a privacy and security audit will be subject to corrective actions.

PROCEDURE:

I. CHNCT's Compliance Officer and Technical Services department will routinely conduct audits to assess the organization's awareness of privacy and security issues.

II. The types of privacy and security audits conducted may include, but are not limited to:
   a. A complete audit of the organization during non-business hours; and
   b. A walk-through of each department during business hours.

III. At a minimum, privacy and security audits will review the following:
   a. **Passwords Displayed**: Any inappropriate displays of system, network ID and/or voicemail passwords will be considered violations. An example of an inappropriate display would be a password written on a post-it note left on a computer or desk.
   b. **Confidential Information Displayed**: ANY inappropriate displays of member information (demographic and health information), employee personnel information, and/or provider credentialing files will be considered violations. An example of an inappropriate display would be

leaving a claim, referral or other communication that has member information on your desk during non-business hours.

c. **Secured Sites**: Areas where confidential information is stored by each employee. Examples of "areas" include filing cabinets, desk drawers, and overhead bins. For those employees who have offices: it is not sufficient to lock your office during non-business hours due to the external cleaning people who have access to all areas. If you keep confidential information in filing cabinets, drawers, etc. these must also be locked.

d. **Computer Security**: A computer that has not been shutdown will be considered a violation (non-business hours only).

IV. CHNCT's Compliance Officer and/or Technical Services department will record and maintain the outcomes of all privacy and security audits and provide summary reports to each Manager.

V. If a deficiency is found, CHNCT's Compliance Officer and/or Chief Information/ Security Officer will discuss the appropriate corrective actions with the applicable Manager. Follow-up audits will be conducted as necessary.