

July 25, 2006

**Policy: Monitoring and Sanctions for Violations of Privacy and Security Policies and Procedures**

Each practice must identify a Practice Liaison. The Liaison or designee will be the Central Network Organization's (CNO's) contact regarding implementing and monitoring this and other network policies.

**Purpose:** To set forth the Northern Berkshire eHealth Summary policy and procedures for the monitoring of patient privacy and data security. This policy and procedure will also address the issue of what sanctions will occur when a violation of patient privacy or data security has been identified.

**Policy:** Any potential violation of eHealth Summary privacy or security policies or procedures by a member of a practice will be identified by:

- 1) a Practice Liaison or designee,
- 2) an interested party, or
- 3) through the audit activity of the CNO.

The potential violation will be documented and investigated. If identified as legitimate, the result will be the sanctioning of the involved practice member(s), up to and including the permanent removal of access rights. The practice member(s) will have the option to appeal the decision.

**Procedure:**

This policy covers all users of the eHealth Summary including employees, providers, volunteers, students and per diem staff members.

1. Prior to providing users with individual IDs, the CNO will provide the Practice Liaison with a copy of this policy, a Confidentiality Agreement, and a User Login form, which will need to be signed by the individual user. These documents outline the expectations that the CNO has regarding maintaining the privacy of the eHealth Summary, explain the monitoring that will take place, and list the sanctions for any violations.
2. The CNO will monitor frequency of eHealth Summary access by user ID and will notify the appropriate Practice Liaison of any unusual activity, including the user ID(s) associated with the activity. The CNO may also audit and report to the Practice Liaison user activity if there is any suspicion that an eHealth Summary privacy violation has occurred (for example, a news story with medical information is published). If the Practice Liaison or designee has not reviewed and either confirmed or denied that access was appropriate within 2 business days (or less for more egregious issues), the CNO may temporarily block network access for the identified user(s).
3. The CNO will keep an audit log of all eHealth Summary activity, including user ID, practice ID, patient file accessed, the extent of the access, and the time and date of the access.
4. Audit logs will be shared with the Practice Liaisons on a monthly basis.

5. Not less frequently than once per year, the Practice Liaison or designee will review the monitoring reports provided by the CNO to conduct random audits of access for each user to confirm their appropriateness, i.e. was the user involved in the preparation, follow-up, or care of the patient whose records were accessed. If inappropriate access occurred, the Practice Liaison or designee will complete a complaint form, including a recommendation regarding the level of violation. The form and recommendation will be forwarded to the CNO.
6. The results of the Practice Liaison's audits and a review of the CNO policies will be conducted periodically, not less frequently than once a year, with the Practice Liaisons or designees from each of the participating entities and the CNO.
7. If a practice member, patient, or other individual has a complaint regarding the inappropriate access or sharing of eHealth Summary information, this complaint should be forwarded to the appropriate Practice Liaison for that user. The complaint will be investigated and either confirmed or denied by the user's Practice Liaison or designee. Complaints may also be filed in writing with the CNO directly, if filing the complaint with the appropriate Practice Liaison is not practical (for example, the complaint is regarding the Practice Liaison or there is fear of retribution). In these instances, the CNO will then notify the appropriate practice administration of the complaint. In either situation, a complaint form detailing the complaint, the outcome of the investigation, and a recommendation regarding level of violation (if appropriate) needs to be filed with the CNO within 2 business days of notification, or less for more egregious issues.
8. Users identified by Practice Liaison(s) as having violated patient privacy or security will be notified that they have the right to protest the findings by submitting a written appeal request to the practice administration. The practice administration will make the final decision and notify the CNO of the outcome.
9. Sanctions consistent with the violation will be imposed on the offender. The practice may have additional sanctions beyond those required by the CNO, i.e. immediate termination or legal action.
10. Sanctions will be in place for Unintentional and Intentional violations:
  - a. Unintentional: Violations and Sanctions

*An accidental breach is often due to lack of education or awareness. Examples include failing to log off a computer, leaving a screen open for others to view, or inadvertently sending information to the incorrect recipient. These breaches may not actually result in the exposure or inappropriate sharing of patient information.*

- i. Initial incident: verbal warning
- ii. Second incident within a year: warning letter from the Practice Liaison and CNO
- iii. Third incident within a year: 30 day suspension from eHealth Summary access
- iv. Fourth incident within a year: removal of network access for six months
- v. Fifth incident within a year: indefinite suspension of network access

b. Intentional: Violations and Sanctions

*An intentional breach is one that occurs due to curiosity, a desire for personal gain, or the intent to harm someone. This includes looking at a friend's or relative's record out of concern. An intentional breach also includes sharing information to damage someone's reputation or livelihood, or selling information to anyone for any reason.*

- i. Indefinite suspension of network access
  - ii. Prosecution to fullest extent of law
11. If multiple practice user violations are reported and/or the CNO has reason to believe that the eHealth Summary is not being kept private or secure by a practice, the CNO may sanction the practice in the following manner:
- i. Warning letter from the CNO
  - ii. 30 day suspension from eHealth Summary access
  - iii. Removal of network access for six months
  - iv. Indefinite suspension of network access
12. On an annual basis, the Practice Liaisons will review these policies with users and obtain a signed acknowledgement.