

August 11, 2006

Policy: Mitigation and Notification of Privacy and Security Violations of the eHealth Summary

Purpose: To set forth the Northern Berkshire eHealth Collaborative’s policy and procedures regarding the mitigation and notification of privacy and security violations of the eHealth Summary (eHS).

Policy: Each practice will mitigate to the extent practicable or applicable any harmful effect that occurs as a result of use or disclosure of eHS information in violation of state and/or federal (HIPAA) policies and procedures or those of the CNO, if the unauthorized disclosure is made by either the practice or any of the practice’s Business Associates.

PROCEDURAL GUIDANCE

A. Notification of CNO of Unauthorized Disclosure:

An unauthorized disclosure of eHS information by a practice or any of its Business Associates shall be reported to the CNO by the practice as outlined in the Northern Berkshire eHealth Collaborative’s Monitoring and Sanctions for Violations of Privacy and Security Policies and Procedures document.

B. Mitigation Plan:

Once the Practice Liaison or its designee has verified that an unauthorized disclosure of eHS information has occurred, a determination then must be made regarding the need for a Mitigation Plan, depending on the type and scope of the unauthorized disclosure. If it is determined that a mitigation action plan is required, the Practice Liaison or designee shall develop and implement a plan as soon as reasonably practicable to minimize any known or reasonably anticipated harmful effects from an unauthorized disclosure (the “Mitigation Plan”). Each Mitigation Plan shall be tailored to the circumstances of each case, and may include, as appropriate, the following:

1. No action necessary other than the reporting of the event to the CNO.
2. Identify. Identifying the source(s) of the unauthorized disclosure and taking appropriate corrective action.
3. Contact. Contacting the recipient of the information that was the subject of the unauthorized disclosure and requesting that the recipient either destroy or return the information.
4. Instruct. Instructing the recipient to make no further disclosure of the information.
5. Notify. If it is determined to be appropriate and warranted, Notification will be provided to individual(s) whose eHS information was the subject of the unauthorized disclosure. Notification is required in circumstances where there has been an unauthorized release of eHS information that may cause personal, financial, or professional harm to the individual(s) involved. For example, once it is recognized that a patient’s address was shared inappropriately with a third party in a domestic abuse situation, the patient should be notified immediately.
6. Review and Correct. Reviewing and correcting where appropriate, any policy or procedure of the practice that directly caused or contributed to the unauthorized disclosure.

A copy of the Mitigation Plan should be submitted to: **eHealth Network Administrator, David Delano, 71 Hospital Ave., Clark House 3rd Floor, North Adams, MA 01247. Fax to: (413) 664-5322. .**