

NORTHCARE NETWORK

POLICY TITLE: ELMER Security Policy

REVIEW/REVISED:

POLICY EFFECTIVE DATE: 11/4/2009

BOARD ADOPTED: 11/4/2009

BOARD APPROVED REVISION:

POLICY STATEMENT

This policy establishes expectations for maintaining the confidentiality, integrity and availability of electronic protected health information (ePHI) in ELMER.

DEFINITIONS

Computing equipment – refers to computers, laptops, personal digital assistants (PDA), smart phones or any other device capable of accessing ELMER

Security Incident – An intentional or unintentional event resulting in an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

EXPECTATIONS

ELMER is a web based electronic health record solution requiring a unique set of technical and non-technical initiatives to maintain the confidentiality, integrity and availability of the system.

NorthCare and the Affiliates shall maintain the following requirements:

1. Maintain accurate and updated user accounts in ELMER and ensure that all ELMER accounts are removed or disabled upon employee termination, employee reassignment or any occasion where access is no longer required;
2. Have a policy and/or procedure detailing how and when user accounts are maintained;
3. Have security access reports reviewed by NorthCare and Affiliate Security Officer periodically to identify misuse of ELMER accounts, access from restricted subnets or other security related incident;
4. Allow access to ELMER by NorthCare or Affiliate users only on NorthCare or Affiliate owned and managed computing equipment;
5. Establish Business Associate Agreements with independent contractor and sub contractors based on the functions needed and restricts access to business associate's computer owned and operated equipment prior to granting access to ELMER;
6. Provide necessary training with independent contractor and sub contractors prior to granting access to ELMER;
7. Maintain security incident processes, in accordance with the Response and Reporting Standard of HIPAA, to effectively mitigate local and inter-affiliate security risks;

8. Provide for initial and ongoing training as needed to adequately inform ELMER users of proper and improper practices as they relate to ELMER;
9. Participate in regional network management and develop a comprehensive network management plan to assist in identifying and rectifying network problems, which may impact the availability of ELMER to NorthCare and the Affiliates;
10. Report ELMER technical support cases to the Pathways' Help Desk or the NorthCare SysAid program promptly for resolution;
11. Adhere to all applicable security and notification provisions of the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) legislation;
12. Allow NorthCare to mediate all security issues between the Affiliates and PCE;
13. Report all security incidents to the NorthCare and Affiliate Security Officers, which impact or have the potential to impact the confidentiality, integrity or availability of NorthCare or another Affiliate information or network infrastructure.