St. Dominic's

Security Access Guidelines for Electronic Health Record (EHR) Use in Non-Hospital Clinics

Applicability

Medical Staff members and their office staff who wish to access St. Dominic Hospital's electronic health records in order to enhance the continuum of healthcare to mutual patients.

Policy

As a courtesy, credentialed providers (and their staff if warranted) and reference laboratory clients are permitted access to St. Dominic's electronic health record or EHR to view pertinent medical record information as it pertains to the functionality of the user's job description.

Establishing a Security Administrator

The System Administrator will be the primary contact related to the clinic's use of St. Dominic's EHR. This individual's responsibilities include:

1. Ensuring users who gain access to St. Dominic's electronic medical record system have received HIPAA privacy and security training.

2. Training users on St. Dominic's electronic medical record system.

3. *Submitting to St. Dominic's IT Department all requests for access to EHR.

4. Keeping an up to date log of all users with access to St. Dominic's electronic medical record.

5. Notifying St. Dominic's of a user's change of employment status immediately for deactivation purposes. (Termination, Retirement, etc)

6. Reporting any and all known or suspected unauthorized uses and disclosures to St. Dominic's Privacy Officer within 5 business days of the disclosure.

*St. Dominic Medical Staff Services will submit to St. Dominic's IT Department all requests for access to EHR related to medical staff members.

Access Procedure

The following procedures should be followed to acquire EHR access.

1. For each clinic, a Security Administrator must be established. The clinic Office Manager is most commonly delegated this responsibility. Once it is decided who will serve as Security Administrator, a Security Administrator establishment form should be completed and submitted. *See Attachment 1*.

2. St. Dominic's IT Security Group will provide via email a confirmation of System Administrator setup including an assigned clinic number.

3. Once a System Administrator has been established, each clinic staff member who is requesting access to St. Dominic's electronic health record must complete an "Access Request Form" *(See Attachment 2)* and "Nondisclosure Form" *(See Attachment 3).*

4. These forms must be submitted to the St. Dominic's Information Technology Department by the Security Administrator.

5. After verification and *approval, the IT Security group or delegate will assign user credentials.

6. Login information and URL will ***only*** be sent to individual users.

7. Security Administrator will be notified that access has been granted. All questions should be directed to the Help Desk at 601-200-4000.

8. EHR users who fail to log on for a period of six months will automatically be deactivated.

*Not all requests for access are guaranteed to be approved. St. Dominic's may limit the number of clinic users who gain access to the EHR.

Permitted and Non-Permitted Uses

1. The Hospitals' EHR shall only be accessed and used solely for the ongoing treatment of Clinic's patients.

2. The Hospital's EHR shall not be used for any other purpose. Prohibited uses include but are not limited to: personal use, solicitation for outside business ventures, campaigns, and political or religious causes.

3. Clinic user(s) are prohibited from accessing his/her own or another individual's health information because of a personal request, personal curiosity or personal reasons.

4. Clinic user(s) are prohibited from password sharing.

Training

Clinic is responsible for providing HIPAA training and education to all affiliated users of St. Dominic's EHR. This training should include appropriate access to the EHR and the terms in the Nondisclosure Agreement. Clinic will provide evidence of training and education of its staff upon Hospital request.

Confidentiality

1. Clinic shall only access the EHR as permitted by this Policy. Clinic's use of and access to EHR is limited to the Clinic's treatment of mutual patients of the Hospital and Clinic.

2. Security access will be granted to individuals while adhering to the minimal necessary standard.

3. Hospital will routinely conduct random and targeted audits of access to Hospital's EHR system. Clinic shall cooperate with the Hospital audits and any resulting investigation that may involve clinic's access.

4. It is the responsibility of Clinic to ensure that unauthorized users are not allowed access to Hospital EHR.

5. Access levels will be established for physicians, clinical staff and office staff respectively, with the understanding while one level may be more extensive than another, user ids and passwords will not be shared between levels. Monitoring of EHR activity will be constant, and those found in violation of this policy will be deactivated.

6. Clinic shall implement and maintain appropriate safeguards to prevent the Use of Disclosure of PHI in any manner other than as permitted by this Policy. These shall include administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI that it receives, maintains, or transmits from the Hospital and as required by law.

Unauthorized Uses and Disclosures

Clinic agrees to abide by HIPAA privacy and security regulations with regards to protection of PHI, and must report any and all unauthorized uses and disclosures to the St. Dominic's HIPAA Officer via phone within 5 business days of the known disclosure and via written notice within 10 business days.

Attn: HIPAA Officer
969 Lakeland Drive, Jackson, MS 39216
601-200-6978

1. Clinic shall provide in such notice the remedial or other actions undertaken to correct the unauthorized Use or Disclosure of PHI.

2. Clinic shall mitigate any harmful effect that is known to the Clinic of a Use or Disclosure of PHI by the Clinic in violation of this Policy.

3. Clinic shall work cooperatively with the Hospital in mitigating and preventing any further unauthorized Use or Disclosure of PHI.

Enforcement

Violations of this Policy may result in deactivation of all EHR accounts assigned to the violating client.