

System

Fairview Health Services

Policy

Confidential Information Access via Information Systems

Purpose:

The purpose of this policy is to provide a mechanism to assure that in accordance with federal and state laws, only those individuals with a legitimate business need are allowed access to Fairview information systems that contain confidential information, including Protected Health Information (PHI).

Policy:

Fairview will strictly monitor and control access into systems that contain confidential information and will be able to demonstrate that users are not accessing confidential information inappropriately.

Internal Users: An authorized internal user is any person who has been authorized to access, create, read, update, and / or delete information created or held by Fairview Health Services. Internal users would generally be defined as members of the Fairview workforce, including employees, credentialed medical staff, students, and volunteers.

External Users: Authorized external users include organizational entities and third parties distinct from Fairview with contractual permissions for information exchange with Fairview such as Business Associates who are performing a service on behalf of Fairview. Authorized external users, Business Associates, and their designated agents are required to comply with Fairview's policies and procedures governing the privacy of patient information.

User Identification and Passwords: The designated / authorized application security administrator is responsible for setting up and distributing user identification codes and passwords that allow access into Fairview's information systems that contain protected health information or confidential information (e.g., Epic, Imagecast, etc.).

Minimum Necessary Access for Internal Users and External Users: Internal users are categorized by access levels appropriate for their job duties. Based on the employee's job duties, the application security administrator will respond to the Application Service Request or other approved method of documentation required for adds, moves and changes, submitted by the employee's manager. Upon receipt of a request for access (generally through the Application Service Request form), the security administrator will review the access level that was requested and provide the employee with access to the minimum necessary information to perform their work. External users will agree to access only the minimum amount of information necessary for them to complete their work.

Authorization for External Reviewer Access: External user requests to access information systems that contain protected health information will be reviewed by the Health Information Management Department (HIM) for

appropriateness. If deemed appropriate, HIM will request a user ID and password from the application security administrator and supply it to the reviewer so they will be able to perform portions of their business operations using electronic information. HIM may also determine that it is more appropriate to provide access to the requested information via a report.

Monitoring: Fairview will utilize the existing available technologies to monitor access to protected health information.

Violations: Suspected inappropriate access will be reported to the employee's manager and the Privacy Director and the user ID may be inactivated until a thorough investigation can be performed. Refer to the Compliance Program Discipline, Corrective Action Process, and Reporting, Investigating and Mitigating Compliance Program Violation policies for guidance on handling the issue. When the violation involves a user not employed by Fairview, the user's employer should be notified so that appropriate documentation and corrective action may be taken.

Definitions:

Confidential data is data that requires protection because of its sensitivity. This includes information such as employee data, financial information, and Protected Health Information (PHI). The release of this data may have negative financial, competitive, legal, or other unbeneficial impacts.

Non-confidential data is data that does not require protection because its disclosure would not expose the organization to financial loss, embarrassment, or legal implications.

Protected Health Information (PHI): The demographic and health information collected from an individual that:

1. Is created or received by a health care provider; and
2. Relates to past, present, or future physical or mental conditions of an individual; the provision of care to an individual; or payment related to the provision of care to an individual; and
3. Identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual.
4. Is transmitted or maintained in any form (electronic, paper, oral).

Procedure:

I. Internal Users

A. Requests for internal users to gain access to information systems or reports that contain confidential information will be managed through the established intranet Application Service Request process (which includes manager approval for access) or other approved process established for providing access. The application security administrator will respond to the individual requests per guidelines established for employee roles.

B. The employee's manager or the application support team will arrange application training for new users.

II. External Users

A. External requests for a user ID and password will be routed to the appropriate entity's HIM department contact. Guidelines for determining if the request needs to go through the HIM department are available from the site's HIM department.

B. The external requesting party will be asked to complete the "[External Reviewer Application Access](#)" form and sign the confidentiality and security statement on the form. This will be routed to the appropriate contact within HIM.

C. HIM will be responsible to ensure that the requesting party is authorized to have access to the information they are requesting.

D. HIM may determine that it is more appropriate to create a printed report or to print a copy of the record for the reviewer. The HIM staff person may also access the record using their own user ID, and operate the computer while the reviewers read the requested information on the computer screen.

E. For approved access requests of a non-urgent nature, HIM will complete an Application Access Request (AAR) or other approved process established for providing access. As a result of the AAR or other approved request process, the security department will then contact the appropriate application security administrator for a user ID and password. HIM will determine the level of access necessary and the length of time that the access codes will remain active for the external reviewer.

F. The security administrator will establish the ID and password and communicate it to the HIM contact for the request. HIM will determine the level of training necessary and will contact the appropriate application team if training is necessary.

G. In anticipation of urgent requests for system access, the application security administrator will provide the HIM department with a number of user IDs that have been prepared in advance. When these IDs are used, HIM will communicate to whom they were assigned and when they should be deactivated.

H. HIM will keep track of all user IDs that have been issued to external reviewers and, when appropriate, will request that they be deactivated.

I. External reviewers must request access for each individual user that will be using the information system. Sharing IDs and passwords is a violation of security policies and will result in revocation of access privileges.

Policy Owner:

Privacy Director

Approved By:

Information Privacy and Security Steering Committee

Date(s):

Date Effective: April 14, 2003

Date Revised: April 27, 2006; May 2009; May 21, 2012

Related Information

[External Access Agreement](#)