Section 4: Information Access Management

Access Authorization Policy & Procedure

Upstate Caring Partners

Section 4.1

HIPAA Status: Addressable

General Statement of Purpose:

The specific intent of this policy is to address activities related to the Agency's computer-based information systems. This policy governs which employee is authorized access to individually identifiable electronic protected health information.

Citation(s):

§164.308(a)(4)(ii)(B)
SHIELD Act S5575B
Parents Bill of Rights; Education 2-D

Policy Statement:

It is the policy of the Agency to provide appropriate employees and volunteers with data and information needed to carry out their duties quickly, efficiently and effectively. Access authorization is the process of determining whether a prospective data user should be granted access to the Agency's data. All employees of the Agency must comply with this policy and demonstrated competence. However, circumstances could result in an override of these procedures when the Vice President of Information Systems and the appropriate manager agree on the reason and the reason is documented. That documentation is also forwarded to the Security Officer.

Definition(s):

Agency: Upstate Caring Partners

Agency record: Any collection of electronic data that must be maintained as per federal, state, local, Agency laws, regulation, or policy.

HIPAA: Health Insurance Portability and Accountability Act of 1996.

IT: Information Technology, which consists of the Division Director of Information Systems or Computer Support Specialist or designee

PHI: Protected Health Information

Procedure(s):

All new hires will receive an email account and a randomly generated password that must be changed on first login. This account will only allow access to email and non-PHI related documentation that is available to all employees.

For each person requesting access to PHI, a "Network Access" form must be completed and submitted to the Information Systems Group. A supervisor's physical signature will be required either in writing or electronic format.

This form will specify:

- What information access is requested (individual records, folders, programs, hardware, etc.).
- Level of access to PHI, such as use (read only or full access).
- The reason why such access is needed (based on "minimal necessary" access).
- The date access is to start.

The request is forwarded to VP Information Systems or Designee (Help Desk). The request will be evaluated as follows by the Network Administrator or designee.

- Verify that the request for ID was received from the persons Direct Supervisor or higher position using the Agency Database – Ulti-Pro and the Agency Organizational Chart.
- Verify that the person getting the access is an active employee through the Agency Database – Ulti-Pro.
- Verify that the supervisor gave a written justification for the access requested.
- Verify the requested level of access.

If the Network Administrator or designee feels that the information is not complete, enough to properly assign the account requested they may take the following action:

- Reject the request pending additional information and ask to have it resubmitted.

Persons not having approved access are prohibited from using Agency computer systems. The ID and password will be emailed through the agency email system to the supervisor or distributed at the orientation to the new hire.

ID specifications:

The id will be the user's first name and first two initials of their last name for internal network use. Conflicts with duplications will be resolved according to the Network Administrators discretion. The user's initial password will be 8 characters long and be generated by a random password generator utility. The user will be instructed on how to change their initial password via a written document emailed to them by the IS department. The password will be a "strong" password containing of numbers, letters and symbols. Routine password changes will not exceed 3-4 months controlled by Active Directory Policy.

Internet e-mail addresses will be in the form of first.lastname@upstatecp.org, first.lastname@cnyhealthhome.net, first.lastname@kelbermancenter.org & first.lastname@ufhcinc.org

Any questions on the interpretation or application of this policy/procedure should be cleared with the Security Officer at UCP.

Sanctions:

Failure to comply with UCP's policy or procedure may result in disciplinary actions, in accordance with Upstate Caring Partners' Human Resources Policy Manual. In addition, a violation of this policy may be a violation of the federal, state, and/or local law. The agency may be required to contact outside authorities to conduct an investigation leading to criminal or civil prosecution.