healthcurrent

Imagine fully informed health

Health Current Information Security Requirements

This document highlights some of Health Current's Information Security Requirements for our Participants using our services.

Account Requirements

HIE Portal and Direct Secure Mail accounts enable access to PHI and should be protected by participants and the owner of the user account. Below are the requirements for using HIE services:

- Do not use a single account to share with a team or other team members. This will protect against potential breaches and allow for reliable auditing of accounts.
- When someone from your organization who has a portal account is terminated, immediately request that their portal account be disabled. Contact HIESupport@healthcurrent.org or contact your assigned Account Manager with the person's name and when you would like the account disabled by.
- If you are working with a vendor who is requesting access to the HIE portal, reach out to an authorized user in your organization who is approved to request access for the vendor or third party. When making the request, include when access should be removed for the vendor or third party.

Password Management

Password Complexity

Passwords are your digital key to access Health Current's portal and services and is the best way to keep information safe. When setting up an HIE portal password we must first understand the complexity rules. Complexity rules are used to make it more difficult to guess or hack passwords. passwords must be at least 8 characters long, contain a capital letter, lower case letter, number, and a special character. Passwords are set to be expired every 90 days.

Password Best Practices

Portal access grants you access to PHI and sensitive data. One of the simplest ways to protect data is using good judgement and safeguarding your access to Health Current services using password best practices.

- Avoid using obvious passwords.
- Use unique passwords such as using a passphrase and using the first letter of each word in the phrase or using special characters. For example: Great to meet you could be Gr82M33tU!
- Refrain from using dictionary words as this is easy for hackers to guess.

healthcurrent

Imagine fully informed health

- Do not include personal information such as your child's or pet's name in the password as they are easy to find on social media.
- Do not reuse passwords. For example, do not use the same password for the portal that you use to log into your network account.
- Do not share your portal password with anyone. Health Current will never ask you for your portal password.

Incident Management

An incident is the act of violating an explicit or implied security or privacy policy. These acts include but are not limited to:

1. Unauthorized use of the portal or services.
2. Using someone else's password or login ID.
3. Unauthorized user access of patient records.
4. Alerts routed to the wrong recipient.

Reporting an Incident

If there is suspicion that an incident is occurring or has occurred, it is important to immediately start recording all facts regarding the incident. Facts are the date and time of the incident, what steps were taken prior to the incident, affected parties, who witnessed the incident, or any relevant facts.

Incidents are time sensitive and should be reported in at least 24 hours since the incident was discovered. The Incident Response team at Health Current will begin investigating the incident with the facts and details provided. Report incidents to your assigned Account Manager or email: HIESupport@healthcurrent.org.