care resource
Your Community's Source for Healthcare

INFORMATION SECURITY AND ACCESS CONTROL

Policy Number
4002.001

Policy Category
Information Services

Target Audience
All Care Resource Employees, Contractors, and Vendors with access to Care Resource Information Systems

Overview
Information security is to ensure the confidentiality, integrity, and availability of information resources and data to reduce the risk of information loss by accidental or intentional alteration, disclosure, or destruction and preserve the health center's protected health information.

Purpose
The purpose of this policy is to protect against unauthorized access, use and disclosure of protected health information along with the risk of loss, damage, unauthorized alteration, unintentional change, and accidental destruction.

Policy
Care Resource understands, acknowledges, and respects the importance of Protected Health Information. Information security is to ensure the confidentiality, integrity, and availability of information resources and data to reduce the risk of information loss by accidental or intentional alteration, disclosure, or destruction and preserve the health center's protected health information. The implementation of information security protects against unauthorized access, use and disclosure of protected health information along with the risk of loss, damage, unauthorized alteration, unintentional change, and accidental destruction. Authorized system users and restricted access system users must keep information obtained.

Procedure

Care Resource may become aware of situations that could place the health center's facilities, employees, critical administrative and clinical functions, and protected health information at risk or harm. These situations include, but are not limited to:

1. Knowledge of existing or potential security violations

2. Knowledge of a situation that may potentially place the health center's critical administrative and clinical information at risk of being lost, altered, or unavailable
3. Terminated employees or other health center representatives who continue to have access to facilities or information technology resources once access is longer warranted or permitted
4. Changes to user access needs which may include employees who transfer to other departments and employee promotions
5. Processes that may place the health center's information at risk
6. Unsolicited requests for Care Resource information from external sources such as questionnaires requesting financial data.

Security Incident Notification

An incident involves any aspect of information technology, which is not part of standard operations and has the potential to cause harm to health center data resources and/or financial loss.

It is the responsibility of all health center to staff to report suspected and/or confirmed incidents. All suspected and/or known violations must be reported to the Information Services department who will report to the appropriate department. All such allegations of misuse will be investigated by the Information Services department and Human Resources.

Security Incident Response

Incidents may occur that require the full participation of Information Services personnel as well as Care Resource leadership to manage the outcome properly. Information Services establishes incident response procedures that adhere to the following minimum guidelines:

- Assess the seriousness of the incident
- Assess the extent of the damage
- Identify the vulnerability created
- Estimate what additional resources are required to mitigate the incident
- Ensure that proper follow-up reporting occurs and that procedures are adjusted so that responses to future incidents are improved

Accounts and network access may be administratively suspended with or without notice by the health center when continued use of IT resources may interfere with the work of others, places the health center or others at risk, or violates Care Resource policy.

Physical security or safety concerns All departments must establish minimal requirements for the access, use, and disclosure of protected health information listed below:

1. All individuals who require access to resources containing protected health information must be appropriately authorized.
2. The authorization will be approved on a need-to-know basis by the relevant manager.
3. Access to information systems must be restricted to authorized staff to prevent and detect unauthorized access or abuse.
4. The use of remote access requires that protected data be secured at all time and must never be moved or copied outside of standard approved operating procedures.
5. Data encryption must be used to secure the health center's data from risks including but not limited to access, use, disclosure, and removal of protected health information.
6. Physical security measures for accessing information resources through physical means including disaster controls, physical access controls, device and media controls, and procedurals controls must be in place.
7. Access to data network facilities and other sensitive areas must be provided on the principle of least privilege and the user's responsibilities.
8. Care Resource may share information with staff, volunteers, licensed independent practitioners, consultants, and partner organizations which have a legitimate role in care.
9. Care Resource may share information with non-partner organizations as required by law or by court orders/subpoenas.

Passwords are an important aspect of computer security. Poorly safeguarding passwords may result in unauthorized access and/or exploitation of resources. All users with access to Care Resource's systems are responsible for taking the appropriate steps, as outlined below, to safeguard their passwords.

1. Passwords must not be written down
2. Passwords must not be communicated to or shared with others.
3. Passwords to core health center systems will be changed on a regular six-month basis.
4. Passwords must be changed immediately upon:
    a. Learning a password has been compromised
    b. A security breach is suspected
    c. Learning a password has been shared with another individual
    d. Changes of personnel or personnel leaving the health center
    e. User no longer requires access to the system

All known and/or suspected violations must be reported to the applicable systems administrator, who will report, as appropriate, to the applicable department. All such allegations of misuse will be investigated by the appropriate department with the assistance of the Information Services and Human Resources departments.

Penalties may include, but are not limited to:

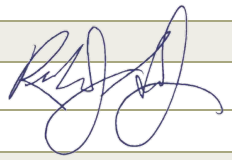
1. Suspension or termination of access to computer and/or network resources
2. Suspension or termination of employment, to the extent authorized by health center published policies and procedures
3. Suspension or termination of contract computer and/or network services
4. Criminal and/or civil prosecution

Enforcement

This policy will be enforced by Management.

Approved by:

- Print and Sign Name Rick Siclari, MBA - CEO



Effective Date

- 05/01/2013

Revised Date

- 06/22/2022

Reviewed Date

- 06/22/2022

Distribution Date

- 06/27/2022