care resource
Your Community's Source for Healthcare

PRIVACY RULES

Policy Number
1014.006

Policy Category
Administrative

Target Audience
All Care Resource Employees

Overview

Care Resource understands, acknowledges, and respects the importance of protecting health information. Therefore, the health center will comply with HIPAA, FIPA, and other Privacy laws and regulations.

Purpose

The purpose of this policy is to outline standard requirements related to HIPAA, FIPA, and other Privacy laws and regulations.

Definition

Breach: unauthorized access of data in all forms (electronic and paper) containing personal information. Good faith access of personal information by an employee or agent of Care Resource does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Policy

- All staff must comply with the Health Insurance Portability and Accountability Act (HIPAA) and Florida Information Protection Act (FIPA) regulations.
- Handling of private health records and other health information must be consistent with privacy regulations.
- Care Resource will develop appropriate written privacy procedures and notices which will be posted in the lobby.
- All staff/volunteers will receive proper training on privacy rules and procedures, as well as on disciplinary actions for failure to comply with such requirements.

- A signed acknowledgment of this training must be placed in the staff/volunteer's Human Resources volunteer or Board record.
- Information about the health center's Privacy Regulations will be available for clients/patients in the form of the "Notices of Privacy Practices" Intake document.
- Standards for safeguarding protected information will be observed, and authorizations for use and disclosure of Protected Health Information will be made available to the health center's clients/patients.

Reporting

- Any occurrences of violation or non-compliance with Privacy Rules must be reported via the Incident Report Form.
- Reporting can and must be done by any employee (including providers and management) who observed or uncovered a suspected violation or non-compliance.
- Care Resource's Privacy Officer will investigate and recommend appropriate remedial and preventive actions.
- Recommended actions must be followed by affected department(s) to resolve, prevent and/or minimize future occurrences. Such actions might include but are not limited to revising policies, developing standard operating procedures (SOPs), training and disciplinary action.
- If a violation of the Privacy Rule is determined to have occurred, the Privacy Officer will investigate the incident and take the appropriate actions. After investigation, if it is determined additional action is needed by Human Resource (HR), the Privacy Officer will refer the incident to HR.
- Care Resource's Privacy Officer will document and log all incident reports and supporting documentation.

Notice of breach will be sent, via mail and/or email, no later than 30 days after the determination of a breach, or reason to believe a breach occurred (unless requested in writing by federal, state, or local law enforcement to extend for a specified period of time). Notification will be sent (if necessary) to external parties or person(s) involved highlighting the following:

  - Date, estimated date, or estimated date range of the breach
  - Purpose of the notice - a description of the accessed information as part of the breach.
  - Contract information for the person to contact for more information regarding the breach.

- Care Resource shall also notify funders' Security Officer, Privacy Officer, and Contract Manager as soon as possible, but no later than four (4) business days following the determination of any breach or potential breach of personal and confidential data. Care Resource shall provide notification to funders' Privacy Officer and Contract Manager within twenty-four (24) hours of notification by the US Department of Health and Human Services of any investigations, compliance reviews, or inquiries by the US

Department of Health and Human Services concerning violations of HIPAA (Privacy, Security Breach). Finally, no later than four (4) business days following a breach, Care Resource shall provide to funders, in writing, sufficient information, provided such information is available, to permit funders to comply with the Breach notification requirements.

- Care Resource, as applicable, at its own cost, shall notify the affected parties no later than thirty (30) days following the determination of any potential breach of personal or confidential data as provided in § 501.171, Fla. Statutes following a HIPAA Breach (Privacy, Security Breach). Care Resource will continue to inform funders of new and material information learned regarding the HIPAA Breach.

- Care Resource will comply with FIPA requirements and notify the FL Department of Legal Affairs for breaches affecting 500 or more people. If 1000, or more people are affected, in addition to notification of the FL Department of Legal Affairs, notice will be sent to all nationwide consumer credit reporting agencies. If a breach is caused by a 3rd party agent, who maintains a security system for the health center, the 3rd party agent has 10 days to report the breach to Care Resource, then Care Resource has 30 days' notice period.

Integrity Controls - Care Resource will implement mechanisms to ensure protected health information is not improperly modified without detection until disposed.

Appropriate safeguards include the use of unique user identification (Password). IT will periodically conduct audits to ensure the integrity and take appropriate actions if changes to electronic protected health information are made without authorization. See Policy No. 4002.001 - Information Security and Access Control.

Mechanisms to authenticate protected health information - Care Resource will implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. It will also implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. The authentication mechanisms will ensure that a person is in fact who he or she claims to be before being allowed access to EPHI. See Policy No. 4002.001 - Information Security and Access Control.

Testing and revisions of plans and analysis of applications- Care Resource will implement procedures for periodic testing and revisions of contingency plans - response to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster). It will also assess the relative criticality of specific applications and data in support of other contingency plan operations. The objective is to assess the healthcare center's capacity to keep its data secure and the risks facing any data stored, received, transmitted in its systems.

See Policy 4001.001 - Clinical Information Management Continuity and Recovery Plan.

Media re-use - Care Resource will implement procedures to ensure that protected and confidential information is permanently rendered unrecoverable from all forms of media before it is disposed or reused. This is to prevent the recovery of data by unauthorized sources.

Disposal of media and devices - Care Resource ensures that media and devices are properly disposed. See Policy No. 4005.003 - Information Technology Asset Management.

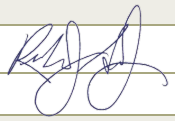
Email of Protected Health Information (PHI) - Care Resource will take reasonable steps to minimize the risk of transmitting PHI to the wrong person or the risk of intercepting email transmitting PHI during transmission. To minimize these risks:

- Specific information regarding highly sensitive Protected Health Information should never be transmitted or received via regular end user email accounts i.e., information relating to AIDS/HIV, drug and alcohol abuse, and psychotherapy notes.
- When it is necessary to transmit PHI to ensure clinicians can efficiently exchange important client/patient care information, the transmission must be done via a Care Resource secured internal network, such as secure messaging via the Patient Portal.
- Information transmitted in an email should be limited to the minimum necessary for clinical purposes.
- The email address should be verified for accuracy prior to transmitting PHI
- The email should always include a privacy statement notifying the recipient of the insecurity of the email and providing a contact to which a recipient can report a misdirected message.

Fax of Protected Health Information (PHI)- Care Resource will not send PHI over Fax unless it cannot be sent over any other, more secure channels i.e., delivery by hand, and secure email. If information must be faxed, the following steps must be taken:

- Information transmitted in a fax should be limited to the minimum necessary for clinical purposes.
- Transmission should include a cover letter, and the cover letter must include a privacy statement notifying the recipient of the insecurity of faxes and providing a contact to which a recipient can report a misdirected message.
- Fax numbers should be verified for accuracy prior to sending all faxes.

Enforcement
This policy will be enforced by Management

Approved by:
• Print and Sign Name Rick Siclari, MBA - CEO 

Effective Date
• 4/14/2003
Revised Date
• 7/21/2023
Reviewed Date
• 7/21/2023
Distribution Date
• 7/25/2023