CONFIDENTIAL DATA

Policy Number
4011.003

Policy Category
Information Management

Target Audience
Information Services Employees / Management

Overview

Confidential data is often the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. Also, certain regulations/industry standards specify how certain types of data must be treated. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

Purpose

The purpose of this policy is to detail how to identify and handle confidential data. This policy lays out standards for the classification and use of confidential data and outlines specific security controls to protect this data.

Scope

The scope of this policy covers all company-confidential data, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

Policy

Data Classification

Information assets are assets to Care Resource just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to company operations and the confidentiality of its contents. Once this has been determined, Care Resource can take steps to ensure that data is treated appropriately.

Of particular concern is confidential data or ePHI. This must be identified and inventoried in all its forms – electronic, printed, or stored on digital media – and segregated from Care Resource's non-confidential data so that access to it can be more tightly controlled and tracked. Any media that contains ePHI must be catalogued

and secured.

Examples of Confidential Data

The following list is not intended to be exhaustive, but should provide Care Resource with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Electronic Protected Health Information (ePHI)
- Medical and healthcare information
- Credit card information
- Employee or customer social security numbers, or other personal information
- Customer data, including customer lists and customer contact information
- Company financial data which has not been released publicly
- Sales forecasts
- Product and/or service plans, details, and schematics
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Any confidential data held for a third-party (be sure to adhere to any confidential data agreement covering such information) and append that agreement, or a summary thereof, to this policy.

Inventory

After classification, identify all systems, devices, and media that house, collect, store, and process ePHI. For each system, determine and document if healthcare clearinghouse functions exist on that system. Determine and document ownership, responsibility, and functions of each system. Remote access devices and removable media must be included in the inventory if they meet the criteria above.

Treatment of Confidential Data

The following sections detail company requirements on the storage, transmission, and destruction of confidential data. Care Resource must determine the access control capabilities of each system housing ePHI to ensure that the standards outlined in this section can be met. If the standards cannot be met with existing infrastructure, Care Resource must acquire and implement additional hardware, software, or procedures to ensure compliance.

Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Hardcopies of confidential information

must be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

Electronic confidential data must be stored only when absolutely necessary, and must always be kept in encrypted form, using strong encryption. Note that this requirement applies to backups containing confidential data as well.

Confidential data must never be stored on non-company-provided systems (i.e., home computers).

Transmission

Securing confidential data, such as ePHI, during transmission (being electronically sent from one device to another), presents a host of security challenges. In order to keep this data secure, Care Resource must take an active role in ensuring the data is protected from interception or alteration. In order to accomplish this, Care Resource must:

- Identify Risks of Data Interception: Care Resource must identify and review scenarios where confidential data may be intercepted or altered during transmission.
- Develop and Implement Transmission Security Procedures: Care Resource must establish a written set of procedures that ensure the security of confidential information such as ePHI. This should include an analysis of tools and methods, and the implementation of said tools/methods as deemed necessary by the Information Security Manager.
- Develop and Implement Integrity Controls: Care Resource must implement procedures that ensure data integrity is maintained throughout the transmission process, as deemed necessary by the Information Security Manager.
- Implement Encryption: Care Resource must secure all confidential data, such as ePHI, during transmission with strong encryption, as detailed elsewhere in this document. Care Resource should require the use of strong encryption by disabling support for weaker encryption schemes. If the transmission occurs as part of a web application, ensure that HTTPS is forced and displayed in the browser URL bar whenever confidential information, such as ePHI, is requested.

Destruction

Media containing confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross-cut shredding or incineration is required in order to make the data unrecoverable. Care Resource uses a HIPAA compliant document shredding service- Shredding Bin Use and Protection Procedure available for reference.
- Storage media (CDs, DVDs): physical destruction is required, via any means that makes the data unrecoverable.
- Hard Drives/Systems/Mobile Storage Media: The strongest commercially available data wiping technology must be used to ensure that the data is

or deleting the data is not acceptable as this does not destroy the data.

Rather than putting the responsibility for data destruction on users, Care Resource may implement a system to ensure that data is destroyed in a manner consistent with this policy. Media awaiting destruction under this policy must be physically secured until the necessary destruction can take place. This can be in the form of a locked cabinet or other secure storage solution.

Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to Care Resource's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data to which they have been granted access. Such data must be marked or otherwise designated "confidential."
- Users must only access confidential data when it is necessary to perform his or her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor. Refer to the Breach Notification Policy for further information.

Sharing Confidential Data

If confidential data is shared with third parties, such as service providers or Business Associates, a written confidential information and/or non-disclosure agreement must govern the provider's use of confidential information. Further, Care Resource must maintain a written agreement with the provider that indicates how the data should be used, secured, and destroyed.

When Care Resource will be sharing confidential data or ePHI with a service provider or other third party, due diligence must always be performed prior to a provider being selected. Further information about sharing ePHI can be found in the Business Associate Policy.

If media containing confidential or ePHI is sent external to Care Resource, rigorous security procedures must be developed and maintained, which will include, at minimum, credential-verification and signature of the backup service courier. Media must be sent via a delivery method that allows the media to be tracked, such as with a tracking number, and records the signature of the receiver.

Removable or other electronic media that is sent internal to Care Resource, such that the media changes locations or traverses security zones, must be documented with A) the reason for the move, B) the person responsible for the data, and C) supervisory approval for the move. Removable or other electronic media that is sent internal to the company, such that the media changes locations or traverses security zones, must be documented with A) the reason for the move, B) the person responsible for the data, and C) supervisory approval for the move.

Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. Care Resource requires that the following guidelines are followed:

- Strong Encryption: Strong encryption must be used for confidential data transmitted external to Care Resource. Confidential data must always be stored in encrypted form, whether such storage occurs on a user system, server, laptop, or any other device that allows for data storage. See the Encryption Policy for more information about strong encryption.
- Network Segmentation: Care Resource must use firewalls, access control lists, or other security controls to separate the confidential data from the rest of the corporate network, and more specifically, to isolate healthcare clearinghouse functions. More detailed information about this can be found in the Network Security Policy section on Network Compartmentalization.
- Physical Security: Systems that contain confidential data, as well as confidential data in hardcopy form, must be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data. Refer to the Physical Security Policy for further guidance.
- Printing: When printing confidential data, the user must use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas or have the capability for providing secure printing.
- Faxing: When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.
- Emailing: Confidential data must not be emailed inside or outside Care Resource without the use of strong encryption. More information can be found in the Email Policy.
- Mailing: If confidential information is sent outside Care Resource, the user must use a service that requires a signature for receipt of that information. When sent inside Care Resource, confidential data must be transported in sealed security envelopes marked "confidential."
- Wireless Access: When confidential data, such as ePHI, is transmitted or accessed via wireless networks, Care Resource must use wireless industry best practices for encryption, such as IEEE 802.11i. Only the strongest encryption algorithms must be used to secure this data during transmission. Please note that the use of known insecure encryption methods, such as WEP, is expressly

prohibited.

- Discussion: When confidential information is discussed it must be done in non-public places, and where the discussion cannot be overheard.
- Display: When confidential data is numerical, such as social security numbers, it must be removed if possible. If necessary for this information to be displayed, it must be masked (i.e., such that only the last four digits are displayed). Please note that this restriction does not apply to employees who must have access to this data to perform their job functions. This requirement does not supersede more restrictive requirements relating to the display of confidential data. Confidential data must be removed from documents unless its inclusion is absolutely necessary.

If confidential data is written on a whiteboard or other physical presentation tool, the data must be thoroughly erased after the meeting is concluded.

- Media: Any media containing confidential information or ePHI must be physically secured in an access-controlled area or high security zone. Media moved from one area to another must be logged with, at minimum, the following information: contact information of mover, reason for move, new location of media, security precaution taken, and proof that management approval was obtained prior to the media being moved. Care Resource must control all aspects of storage and accessibility of media, including storing media in secured areas, maintaining inventory logs of media, and conducting annual inventories of all media.

Applicability of Other Policies

This document is part of Care Resource cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

Enforcement

This policy will be enforced by the Information Security Manager and/or Senior Management Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, Care Resource may report such activities to the applicable authorities.

Approved by:

- Print and Sign Name Rick Siclari, MBA- CEO

Effective Date
• 2/23/2021
Revised Date
• 4/14/2023
Reviewed Date
• 4/14/2023
Distribution Date
• 4/25/2023