OPS-CM 541: HIPAA Security

Administrative Signature: _____
[enter name and title]

Date: July 13, 2022
Revised Date: March 28, 2023

PURPOSE

The purpose of this policy is to provide guidelines for the safeguarding of Protected Health Information (PHI) at Crisis Preparation & Recovery, Inc. (CPR, Inc.) and to limit unauthorized disclosures of PHI that is contained in a client's medical record, while at the same time ensuring that such PHI is easily accessible to those involved in the treatment of clients.

POLICY

According to HIPAA guideline 45 CFR §164.310(c), a covered entity must "implement physical safeguards for all workstations that access PHI to restrict access to authorized users." Furthermore, HIPAA guideline 45 CFR §164.310(b) states that a covered entity must "implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or electronic device that can access PHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices)."

The policy of CPR, Inc. is to ensure that PHI is not intentionally or unintentionally used or disclosed in a manner that would violate the HIPAA Privacy Rule or any other regulations governing confidentiality and privacy of health information. The following procedures are designed to prevent improper uses and disclosures of PHI and limit incidental uses and disclosures of PHI that are, or will be, contained in a client's medical record. All employees are responsible for the security of PHI in and out of the workplace.

DEFINITIONS

Availability: The property that data or information is accessible and useable upon demand by an authorized person.

Breach*:* The acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA, which poses a significant risk of financial, reputational, or other harm to the affected individual.

Confidentiality*:* The property that data or information is not made available or disclosed to unauthorized persons or processes.

Double Lock: The CPR, Inc. ideal method of securing PHI is through two methods of protection. Examples include the following:

- Locking paper PHI in a car (single lock) within the locked glove compartment (double lock).
- Storing a document containing PHI on a password-protected computer (single lock) within "My Drive" in Google Drive (double lock).
- Securing a document containing PHI on a password-protected laptop (single lock) within a locked case (double lock).
- Locking paper PHI in a locked building or room (single lock) within a locked cabinet (double lock).

Encryption*:* The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

ePHI*:* Electronic protected health information (see Protected Health Information below).
The Health Information Technology for Economic and Clinical Health Act (HITECH) Act: Part of the American Recovery and Reinvestment Act of 2009 (ARRA); widens the scope of privacy and security protections available under HIPAA and increases the potential legal liability for non-compliance; and it provides for more enforcement.

HIPAA: The federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

Integrity*:* The property that data or information have not been altered or destroyed in an

unauthorized manner.

"Minimum-Necessary" Standard: When PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Department of Labor;
- Uses or disclosures required by law; and/or
- Uses or disclosures required to comply with HIPAA.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Unsecured*:* Any protected health information that has not been encrypted or has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the U.S. Department of Health and Human Services (HHS).

GUIDELINES

Computer access

1. Only employees who need to use computers to accomplish work-related tasks shall have access to computers or laptops.

2. CPR, Inc. Management shall determine which employees have access to which software and devices based on job title and duties and document as such.
3. Access to CPR, Inc. software and devices can be modified, revoked, or granted at any time due to employment changes (i.e. termination, change in job duties or position, etc.).
4. All users of computer equipment must have unique logins and passwords.
5. Posting, sharing and any other disclosure of passwords and/or access codes to anyone other than the Data Integrity and Information Technology Manager and executive leadership is forbidden**.**
6. Access to computer-based PHI shall be limited to employees who need the information for treatment, payment or health care operations.

Printers, copiers and fax machines

1. Printers will be located in areas not easily accessible to unauthorized persons.
2. Documents containing PHI will be promptly removed from the printer, copier, or fax machine and placed in an appropriate and secure location.
3. Any PHI left on a printer, copier, or fax machine at the end of the day will be placed in a designated locked area until the following business day (i.e. cabinet, desk).
4. Unclaimed PHI within 48 hours *may* be disposed of in a secure shredding bin.

Written/Paper PHI

1. All written/paper PHI in the workstation shall be kept out of sight when unattended during business hours.
2. CPR staff will lock written/paper PHI at the end of the day in an appropriate location (i.e. desk, file drawer).

    a. For off site locations, staff will attempt to double lock (see definitions) PHI.

3. All unnecessary written/paper PHI will be disposed of in a personal or CPR shredding bin by close of business.

a. For off site locations that do not have shredding bins, staff will attempt to double lock this PHI until it can be disposed of in a shredding bin at a CPR location in the future.

4. Fax cover sheets should *not* contain any PHI.

ePHI

1. Secure all ePHI by logging off or locking the computer or laptop when unattended.
2. CPR, Inc. recommends double locking all documents containing PHI by saving and storing these documents in Google Drive and removing them from all computer or laptop drives as soon as possible.
3. PHI *cannot* be sent via text messages but *can* be sent via company email or by phone.
4. Phones containing PHI via email must be locked when not in use or unattended.
5. All unnecessary PHI on phones, laptops, or computers should be erased as soon as possible.
6. Computer and laptop monitors shall be positioned so that unauthorized persons cannot easily view information on the screen. If this is not possible on site, a privacy filter may be implemented to limit unauthorized access.
7. Emailing PHI is only permitted through the use of a staff member's CPR account through google mail. PHI should never be transmitted through a personal email account.

Transportation of PHI

1. Transportation of written or ePHI is allowable under HIPAA as long as all reasonable measures are used to ensure the privacy and security of PHI.
2. Staff will maintain PHI in their possession at all times in the community.
3. If necessary to leave PHI unattended in the community (i.e. vehicle, home), staff will make reasonable attempts to lock PHI in a case, or use the double lock method.

Communication of PHI

1. All communication of PHI must fall within the “minimum-necessary” standard (see definitions).
2. Discussion of PHI in public areas or in the presence of unauthorized individuals should be avoided whenever possible.
3. Staff will take reasonable measures to assure that unauthorized persons do not overhear conversations involving PHI. Reasonable measures may include:

    a. Lowering the voice;
    b. Moving to a more private area before continuing the conversation;
    c. Using noise machines outside of offices with poor sound insulation.

PROCEDURES

Departure of employment

1. Staff access privileges will be removed promptly following their departure from employment.
2. Staff will turn in all CPR owned devices (i.e. cell phones, laptops) upon their departure from employment to their supervisor for disposal of PHI by the Data Integrity and Information Technology Manager.

Notification of HIPAA Breach

1. All staff are required to notify the QM department if there is a suspected or observed HIPAA Security Breach.
2. The following are *exceptions* to a breach and do not have to be reported:

    a. Unintentional internal use, in good faith, with no further use (i.e. client record put on the wrong desk);
    b. Inadvertent internal use within job scope (i.e. looking up the wrong client in MacPractice due to a similar name); and
    c. Information that cannot be retained.

3. All breaches *not* meeting an exception above are reported to the QM Department for discussion and final determination.

4. According to the HITECH Act, all clients will be notified of any unsecured breach within 60 days by first-class mail or email (if client prefers) with the following information:

    a. Brief description of the breach;
    b. Description of the type of information involved in the breach;
    c. Steps the client should take to protect themselves from potential harm;
    d. Brief description of how CPR is addressing the breach; and
    e. Quality Management Department contact information for the client if there are further questions.

5. The U.S. Department of Health and Human Services (HHS) must be notified by using the following link:

    https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

    a. If the breach affects fewer than 500 clients, complete within 60 days of the end of the calendar year in which the breach was discovered.
    b. If a breach impacts more than 500 clients, complete without unreasonable delay and no later than 60 calendar days following the discovery of the breach.

6. If the breach affects more than 500 clients, prominent media outlets serving the State or jurisdiction involved are required to be notified with the same information as the client within the same time frame (60 days).
7. QM and staff will follow the “CPR, Inc. HIPAA Breach Process” Protocol.
8. If an employee wishes to report a HIPAA Breach to an outside entity, the U.S. Department of Health and Human Services (HHS) can be notified at the above link, by email at OCRComplaint@hhs.gov; by mail at the U.S. Department of Health and Human Services, 90 7th St, Suite 4-100, San Francisco, CA 94103; by mail at (800) 368-1019; or by fax at (415) 437-8329.

Other HIPAA

1. The following informal CPR, Inc. HIPAA policies and procedures are in place:

    a. Security management process
    b. Assigned security responsibility

c. Information access management
d. Security awareness and training
e. Security incident procedures
f. Contingency plan
g. Evaluation
h. Facility access controls
i. Access controls
j. Audit controls
k. Person and entity authentication.

ACCOUNTABILITY

Employees are responsible for:

- Following policy guidelines and procedures to ensure HIPAA compliance
- Report HIPAA breaches as indicated in above policy to Supervisor and QM department
- Complete annual HIPAA trainings

Managers are responsible for:

- Ensure employees are remaining in compliance with policy
- Notify QM department of HIPAA breach and/or concerns of HIPAA breach
- Ensure supervisees complete mandatory HIPAA trainings

HR is responsible for:

- Providing guidance and support to managers for appropriate intervention when/if employee/manager are consistently out of compliance with above policy.