Family Partnerships of Central Florida

PROCEDURE

Series:	**Operating Procedures**	**COA: RPM 5** **CFOP: 60-17n Ch 7**
Procedure Name:	HIPAA Breach Response	
Procedure Number:	OP-1230	
Review Date:	4/16/24	
Revision #/Date:	N/A	
Effective Date:	01/10/2023	
Applicable to:	Family Partnerships of Central Florida (FPoCF) Board of Directors, All FPoCF Staff, Officers, and Contracted Providers	

SUBJECT: HIPAA Breach Notification Procedures

PURPOSE: This operating procedure establishes a uniform process for notification to the HIPAA Privacy Officer by the Department and its Business Associates when an impermissible or unauthorized acquisition, access, use, or disclosure of PHI or ePHI has occurred which compromises the security or privacy of such information.

References

Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Title 45 C.F.R. Subparts 160, 162 and 164, Security and Privacy of Individually Identifiable Health Information.

Sections 13400, 13402, 13410 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA) enacted February 2009.

2013 HIPAA Omnibus Rule – 78 FR 5566, No. 17.

Definitions

Breach. Section 13400(1) of the HITECH Act defines ‘‘breach’’ as the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

1. Where an exception applies there is no duty or obligation to give notice of a breach.
2. If protected health information is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR

42740, 42742), then it is not a breach, and no breach notification is required following an impermissible use or disclosure of the information. Reporting the issue to the Senior Executive of Data Analytics and Information Technology/HIPAA Privacy Officer or designee is still required.

Inadvertent Disclosure. The access, or use of protected health information from one person authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated person at the same facility and the information received is not further acquired, accessed, used, or disclosed without authorization by any other person (section 13400(1)(B)(ii) and (iii) of the HITECH Act). c. Unauthorized Disclosure. The access, or use of protected health information by an unauthorized person to whom protected health information is disclosed in an instance where such January 6, 2014, CFOP 60-17, Chapter 7 7-2 person would not reasonably have been able to retain the information (section 13400(1)(A) of the HITECH Act).

Unintentional Acquisition. The access, or use of protected health information by an employee or other person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such person with the covered entity or business associate and such information is not further acquired, accessed, used, or disclosed by any other person (section 13400(1)(B)(i) of the HITECH Act).

POLICY/PROCEDURE:

Covered entities and business associates that hold, use, or disclose unsecured “Personal Health Information” (PHI) have a legal duty to notify certain parties in the event of a breach.

This policy establishes a uniform requirement to inform individuals when their unsecured protected health information has been improperly used or disclosed and may lead to financial damage, harm to the individual’s reputation, or other harm. This policy is designed to meet the HIPAA regulations as updated on January 25, 2013.

Overview: If a breach occurs, Family Partnerships of Central Florida (FPoCF) will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed. Business associates of FPoCF must, after discovery of a breach, notify FPoCF of the breach and let FPoCF know the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed. A breach of more than 500 records must also be reported to local media outlets and immediately to Health and Human Services (HHS).

Discovery of Breach: A breach of unsecured PHI shall be treated as “discovered” as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization, (includes breaches by the organization’s business associates). FPoCF shall be deemed to have knowledge of a

breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or business associate of the organization. A Ransomware incident will be considered a Breach unless proven otherwise during incident assessment.

Breach Investigation: The Senior Executive of Data Analytics and Information Technology/HIPAA Privacy Officer or designee shall function as the investigator of the breach. The investigator is responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate. The investigator is the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.).

Risk Assessment: To determine if an impermissible use or disclosure of PHI constitutes a breach, the organization will perform a risk assessment to determine if there is significant risk of harm to the individual. The risk assessment shall be fact specific and address:

1. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
2. The type and amount of PHI involved.
3. The potential for risk of financial, reputational, or other harm.
4. The extent to which the risk to the protected health information has been mitigated.

Delay of Notification: If a law enforcement agency officially requests that a notification, notice, or posting be delayed because it would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed.

Timeliness of Notification: The notice shall be made without unreasonable delay and in no case later than 30 calendar days after the discovery of the breach by the organization involved or the business associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

Content of Notice:
The Notice shall be written in plain language and includes:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
3. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the organization is doing to investigate the breach, to mitigate individual harm, and to protect against further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.
6. In the case of insufficient or out of date contact information for an individual the company will make a public notice via local media outlets.

Methods of Notification:

1. For incidents where there are less than 500 records breached, Individuals must be notified by 1st Class Mail. Reports of breaches affecting fewer than 500 individuals are due to the Secretary (http://transparency.cit.nih.gov/breach/index.cfm) no later than 60 days after the end of the calendar year in which the breaches occurred.
2. A breach of more than 500 records must be reported to Individuals as noted above, the local media outlets and immediately to HHS. Web site to notify HHS: http://transparency.cit.nih.gov/breach/index.cfm
3. Ransomware incidents will additionally be reported to the FBI and the Secret Service as criminal activities.

Breach Log:

The organization maintains a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information is collected / logged:

1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
3. A description of the action taken regarding notification of patients regarding the breach.
4. Documentation of these actions is maintained as required by Federal and State law.

BY DIRECTION OF THE PRESIDENT AND
CHIEF EXECUTIVE OFFICER:

PHILIP J. SCARPELLI
President and Chief Executive Officer
Family Partnerships of Central Florida

Signature Date: 04/17/2024