PROCEDURE

Series: **COA: RPM 5**
CFOP: 50-2, 50-22

Procedure Name:	Breach Procedure
Procedure Number:	OP 1228
Reviewed Date:	N/A
Revision #/Date:	N/A
Effective Date:	09/01/21
Applicable to:	All BFP Family of Agencies (BFP FOA) Staff and Providers

PURPOSE:

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.

PROCEDURE:

References: Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Title 45 C.F.R. 164.308(a)(6)(ii) Response and Reporting

Definitions none

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

Overview: If a breach occurs, Brevard Family of Partnership (BFP) will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed. Business associates of BFP must, after discovery of a breach, notify BFP of the breach and let BFP 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). The organization 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 BFP Director of Contracts and Compliance or designee shall act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as

appropriate. The investigator shall be 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 need to 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 60 (30 if required to FL) 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 will include.

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 harm to individuals, 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 shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be 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 clients 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 shall be maintained as required by Federal and State law.

BY DIRECTION OF THE CHIEF EXECUTIVE OFFICER:

PHILIP J. SCARPELLI
Chief Executive Officer
Brevard Family Partnership / Family of Agencies

APPROVAL DATE: 10/19/21