Agency Wide Policy and Procedure

SECTION: Corporate Compliance	**ATTACHMENT:**
SUBJECT: HIPAA Breach Notification Policy	**APPROVAL DATE: 1/2022**
POLICY NUMBER: 7.11	**REVISION DATE:**

POLICY STATEMENT

Any impermissible use or disclosure of PHI shall be considered a breach and such breach shall be treated as discovered on the date the organization knows, or by exercising reasonable diligence, should have known of the impermissible use or disclosure. Upon discovery of a potential breach of PHI the organization shall conduct an investigation, conduct a risk assessment and based on the results of that risk assessment, determine what, if any, notifications are required as a result of the use or disclosure of PHI.

DEFINITIONS

Breach: The acquisition, access, use or disclosure of Protected Health Information (PHI) in a matter not permitted under the Privacy Rule which compromises the security or privacy of the PHI. Each such use or disclosure is presumed to be a breach unless the organization, or its business associate, demonstrates there is a low probability the PHI has been compromised based on a risk assessment utilizing the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the protected health information or to whom the disclosure was made.
3. Whether the protected health information was acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

The following do not constitute a breach or impermissible use or disclosure of PHI:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access or use was made in good faith within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule;

3. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Disclosure: The release, transfer, provision of, access to or divulging in any manner of information outside the organization.

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a territory, political subdivision of a state or territory who is empowered by law to conduct or investigate an official inquiry into a potential violation of law, or prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

Organization: For the purposes of this policy, the term organization shall mean all departments/programs within First Resources Corp.

Protected Health Information (PHI): Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Unsecured PHI: PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons using technology or methodology specified by the secretary in the guidance issued under section 13402(h)(2) of public law 111-5.

PROCEDURE

1. Investigation: Upon discovery of a potential breach of PHI, the Integrity Officer, or a designee, shall act as the investigator of the breach. The individual assigned to investigate will be responsible for conducting a breach investigation, completion of a risk assessment and coordination of efforts as they relate to security incident response, risk management, public relations, legal counsel, and notification. All documentation related to the investigation, including the risk assessment and notifications made shall be retained for a minimum of 6 years.

2. Risk Assessment: A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures does not violate the Privacy Rule and would not constitute a breach. An acquisition, access, use or disclosure in a manner not permitted is presumed to be a breach unless the organization, or its business associate if applicable, demonstrates there is a low probability the protected health information has been compromised based on a risk assessment based on the 4 factors set forth in the definition of breach.

3. The organization shall maintain documentation showing how the risk assessment was conducted and the outcome of the assessment process. Based on the outcome of the

risk assessment, the organization will determine what, if any, notifications are required. In the event the organization decides to do so, notification of a breach may be made without completing a risk assessment.

4. Notification: If determination is made that breach notification is required pursuant to this policy and applicable laws, all such notices shall be made no later than 60 calendar days after the date of discovery of the breach. The foregoing notwithstanding, if a law enforcement official indicates notification would impede a criminal investigation or cause damage to national security, the organization shall:

    a) Follow any written statement that specifies the time for which a delay is required and delay such notification for the time period specified by the official.

    b) If the request from the law enforcement official is made orally, the organization shall document the statement including the identity of the official making the statement and delay making the notification for a maximum of 30 days from the date of the oral statement unless a written statement is subsequently provided to the organization within 30 days.

5. Notification: The written notification provided in the event of a breach must contain the following information:

    a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

    b) 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, Medicare/Medicaid number, diagnosis or other types of information were involved).

    c) Any steps the individual should take to protect themselves from potential harm resulting from the breach.

    d) A brief description of what the organization is doing to investigate the breach and to mitigate harm to individuals and protect against further breaches.

    e) Contact procedures for individuals to ask questions or to learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.

6. Method of Notification:

a) To the Individual: Written notification shall be made promptly by first class mail to the individual at the last known address of the individual or, if the individual agrees to an electronic notice and such agreement has not been withdrawn, by electronic mail. If the organization knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to the next of kin or personal representative shall be carried out.

7. Substitute Notice: In a situation where there is insufficient or out of date contact information, a substitute form of notice reasonably calculated to reach the individual shall be provided.

   a) In a case where there is insufficient or out of date contact information for fewer than 10 individuals, the substitute notice may be provided by an alternative form of written notice, telephone or other means.

   b) In the situation where there is insufficient or out of date contact information for 10 or more individuals, the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organizations website or a conspicuous notice in a major print or broadcast media in the organizations geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll free number that remains active for at least 90 days where an individual can learn whether his or her PHI may have been included in the breach.

8. Notice to Media: In the event the breach of unsecured PHI impacts 500 or more individuals, notice shall be provided to prominent media outlets serving the state and regional area in which the individuals reside. This notice shall be provided in the form of a press release and shall be distributed to the prominent media outlet as determined based on the state or jurisdiction where the impacted individuals reside.

9. Notice to the Secretary of HHS:

   a) For breaches involving 500 or more individuals, the organization shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

   b) For breaches involving less than 500 individuals, the organization will maintain a log of the breaches and shall report such breaches during the calendar year, or no later than 60 days after the end of the calendar year in which the breaches were discovered.

10. Business Associates: In the event the breached associate of the organization accesses, creates, maintains, retains, modifies occurs through a business associate of the organization, that business associate shall, without unreasonable delay, and in no case later than 30 calendar days after discovery of a breach, notify the organization of such

breach. The notice provided by this business associate shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during such breach. The business associate shall provide the organization with any other information the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon receiving notification from a business associate of a breach, the organization will be responsible for notifying impacted individuals unless otherwise agreed upon by the business associate and the organization.

11. Corrective Action: As part of any breach investigation, determination will be made as to whether disciplinary actions, pursuant to the organizations progressive discipline policy, is warranted. The organization shall apply appropriate sanctions against members of the workforce who fail to comply with the privacy policies and procedures of the organization.

12. Training: All members of the organization's workforce shall be trained on policies and procedures relating to PHI as necessary and as appropriate for employees to carry out their job responsibilities.

13. Applicable Laws:

    42 CFR Part 2
    45 CFR 164.103
    45 CFR 164.304
    45 CFR 164.402
    45 CFR 164.503
    45 CFR 164.530