	UNIFIED FIRE AUTHORITY **ORGANIZATIONAL POLICY MANUAL**	
	Affiliation: Compliance and Records Division Policies	
	Title: **Breach Notification Policy** Number: **200 – 110**	
	Approved: 6/13/2023	By: Fire Chief Dominic Burchett
	Last Reviewed: 4/14/2025	By: Shelli Fowlks Records Mgr.

DEFINITIONS:
See UFA Policy and Procedure - General Compliance and Records Definitions

***Breach*:** A breach is the acquisition, access, use, or disclosure of unsecured protected health information (PHI) in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which compromises the security or privacy of the PHI.

An acquisition, access, use, or disclosure of PHI created, received, maintained or transmitted by UFA that is not permitted by HIPAA is presumed to be a breach unless UFA demonstrates that there is a low probability that the PHI has been compromised based on a "risk assessment" of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Examples of potential breaches:

- UFA laptop, which contains the e-PHI of patients of UFA, is lost or stolen, and an unauthorized party could access the data on the laptop.
- Patient care report (PCR) or electronic health record (EHR) containing health information of a patient of UFA is lost or misplaced, and there is reason to believe an unauthorized party could view the information.
- An employee of UFA accesses the electronic health record (EHR) of his/her neighbor to snoop on the neighbor's medical history.

A breach does not include any of the following:

- Unintentional acquisition, access, or use of unsecured PHI by an employee at UFA or someone acting under the authority of UFA if the acquisition, access, or use was made in good faith and within that individual's scope of authority, so long as the information was not further used or disclosed in violation of HIPAA.
- Any inadvertent disclosure of PHI by an employee who is generally authorized to access PHI to another person at UFA, who is generally authorized to access PHI, so long as the information received as a result of such disclosure was not further used or disclosed in violation of HIPAA.

Policy distributed:

- A disclosure of PHI where UFA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably be able to retain the information.

LEADERS INTENT:
Unified Fire Authority (UFA) is committed to protecting the privacy of our patients and conducting our business operations in compliance with all applicable laws and regulations. Under the Health Information Technology for Economic and Clinical Health Act (HITECH) and the regulations at 45 C.F.R. Part 164, Subpart D, UFA has an obligation following the discovery of a breach of unsecured PHI, to notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed. In addition, UFA has an obligation to notify the Department of Health and Human Services (HHS) of all breaches. In some cases, UFA must notify media outlets about breaches of unsecured PHI. This policy details how we will handle and respond to suspected and actual breaches of unsecured PHI.

POLICY:
This policy applies to all UFA employees who encounter PHI. All suspected breach incidents will be brought to the attention of the UFA Records Manager/Compliance Officer. Each incident will be investigated, and the appropriate response will be initiated.

1.0 Reporting a Suspected Breach Incident

1.1 All UFA employees are responsible for immediately reporting a suspected breach incident to their immediate supervisor or the UFA Records Manager/Compliance Officer. All employees will report all known and suspected HIPAA violations.

1.2 The supervisor will immediately notify the Records Manager/Compliance Officer about the incident and convey all information that is known about the incident.

1.3 The Records Manager/Compliance Officer will document the date that the suspected breach of unsecured PHI occurred (if known) and the date(s) on which the supervisor and the Compliance Officer were notified about the incident.

2.0 Investigating a Suspected Breach Incident

2.1 After making notifications, the Records Manager/Compliance Officer will initiate an investigation to determine whether an actual breach occurred and what actions, if any, are necessary. The Records Manager/Compliance Officer will involve the Chief Legal Officer and the Assistant Chief of Administration and Planning in making these determinations.

2.2 The Records Manager/Compliance Officer will interview all necessary parties who may have information about the incident. The employee who reported the suspected incident and other members with knowledge of the incident may be asked to complete the “Security/Breach Incident Form.” Employees are required to convey all information that they know about the incident and to cooperate in any subsequent investigation regarding the incident.

Policy distributed:

2.3 After gathering all available information about the incident, the Records Manager/Compliance Officer will conduct an analysis to determine whether an actual breach of unsecured PHI occurred. The Records Manager/Compliance Officer will work with the Chief Legal Officer and the Assistant Chief of Administration and Planning in making this determination.

2.4 If it is determined that a breach of unsecured PHI did **not** occur, the reasons behind that conclusion will be thoroughly documented.

2.5 If it is determined that a breach of unsecured PHI did occur, the reasons behind that conclusion will be thoroughly documented. The Records Manager/Compliance Officer will then notify all necessary parties in accordance with this policy.

3.0 Breach Notification to Affected Individuals

3.1 Following the discovery of a breach of unsecured PHI, the Records Manager/Compliance Officer will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach. The Records Manager/Compliance Officer will be the party who is primarily responsible for making proper notice, in consultation with the Chief Legal Officer and the Assistant Chief of Administration and Planning.

3.2 A breach will be treated as discovered by UFA as of the first day on which the breach is known, or, by exercising reasonable diligence would have been known to UFA or its agents.

3.3 UFA will provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

3.4 If a law enforcement official states to UFA that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, UFA will:

3.4.1 Delay notification for the time period specified by the official if the statement is in writing and specifies the time for which a delay is required; or

3.4.2 If the notice is a verbal statement, delay notification temporarily, and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time. If the statement is made orally, the Records Manager/Compliance Officer will document the statement, including the identity of the official making the statement.

3.5 UFA will provide written notification, in plain language, by first class mail to each affected individual at the last known address of each individual. If the affected individual agrees to electronic notice, UFA may provide notice by electronic mail. Notification may be provided in one or more mailings as information becomes available.

Policy distributed:

3.6 The Records Manager/Compliance Officer will send a notice to the affected individuals. The notice will include, to the extent possible:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what UFA is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which will include a telephone number, an e-mail address, website, or postal address.

3.7 If it is determined that the affected individuals need to be contacted immediately to protect them from potential harm, the Records Manager/Compliance Officer will contact those individuals by telephone or other means as soon as possible. In addition, a written notice will be sent to the individuals.

3.8 If UFA knows, the individual is deceased and has the address of the next of kin or personal representative of the individual, UFA will provide written notification by first class mail to either the next of kin or personal representative.

3.9 If UFA has insufficient or out-of-date contact information for any affected individual, UFA will use a substitute form of notice, that in the informed opinion of the Records Manager/Compliance Officer, will reach the individual. Substitute notice is not required in cases where there is insufficient or out-of-date contact information for the next of kin or personal representative of a deceased individual.

3.9.1 If there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone, or other means.

3.9.2 If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice will: (i) be in the form of either a conspicuous posting for 90 days on UFA's home page of its website, or conspicuous notice in major print or broadcast media in geographic areas where the individual likely resides; and (ii) include a phone number for UFA that remains active for at least 90 days where individuals can learn whether their unsecured PHI may be included in the breach.

4.0 Breach Notification to the Media

4.1 For a breach of unsecured PHI involving more than 500 residents of a single state or jurisdiction, UFA will notify prominent media outlets serving the state or

jurisdiction about the breach. The UFA Public Information Officer will be the party in charge of making such notification in consultation with the Chief Legal Officer, Records Manager/Compliance Officer, Assistant Chief of Administration and Planning and UFA Command Staff.

4.2 Notification to the media will be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

4.3 Notification to the media will include all information that must be included in individual notice.

5.0 Breach Notification to HHS

5.1 For breaches of unsecured PHI involving 500 or more individuals, UFA will provide notice to HHS when it provides notice to affected individuals. Notice must be provided in the manner specified on the HHS Website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/. The Records Manager/Compliance Officer will be responsible for ensuring the notice is submitted to HHS in consultation with legal counsel, the Assistant Chief of Administration and Planning, and Command Staff before submitting the information to HHS.

5.2 For breaches of unsecured PHI involving less than 500 individuals, UFA will maintain a log of such breaches. The Records Manager/Compliance Officer will track these breaches on UFA's "Log for Tracking Breach Incidents." UFA will provide information regarding such breaches to HHS annually, no later than 60 days after the end of the calendar year. This will be done in the manner specified on the HHS Website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/. The Records Manager/Compliance Officer will be responsible for ensuring the information is submitted to HHS by March 1st, of each year in consultation with legal counsel and the Assistant Chief of Administration and Planning before submitting the information to HHS.

6.0 Administrative Requirements

6.1 UFA will record and maintain thorough records of all activities related to suspected and actual breach incidents. The Records Manager/Compliance Officer will be primarily responsible for documentation of these activities.

6.2 In the event of a suspected crime or other unlawful activity, local, state, or federal law enforcement may need to be notified. That determination will be made by Command Staff with recommendation from the Chief Legal Officer, the Assistant Chief of Administration and Planning, and the Records Manager/Compliance Officer.

6.3 UFA will train all members of its staff, to be able to identify suspected breaches of unsecured PHI and know to report all suspected breaches to the appropriate party immediately.

Policy distributed:

6.4 Employees who violate this policy will be subject to disciplinary action, up to and including termination.

Replaces policy dated July 15, 2019

Policy distributed: