



**City of Winchester  
Fire & Rescue Department  
STANDARD OPERATING PROCEDURE**



<b>Section:</b>	HIPAA	<b>SOP:</b>	14.7
<b>Subject:</b>	Notification of Breaches of Unsecured Protected Health Information	<b>Executed:</b>	May 28, 2015
		<b>Revised:</b>	
<b>Approved:</b>			
 Allen W. Baldwin, Fire Chief			

**Purpose**

Under the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) Winchester Fire & Rescue has an obligation, following the discovery of a breach of unsecured protected health information (“PHI”), to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed. Winchester Fire & Rescue also has an obligation to notify the Department of Health and Human Services (“HHS”) of all breaches. In some cases, Winchester Fire & Rescue must notify media outlets about breaches of unsecured PHI. This policy details how Winchester Fire & Rescue will handle and respond to suspected and actual breaches of unsecured PHI.

**Scope**

This Policy applies to all Winchester Fire & Rescue staff members who come into contact with PHI. All suspected breach incidents shall be brought to the attention of their direct supervisor and HIPAA Compliance Officer/EMS Billing Manager. Together, this team will investigate each incident and initiate the appropriate response to the incident.

**Procedure**

***Reporting a Suspected Breach Incident***

1. All Winchester Fire & Rescue staff members are responsible for immediately reporting a suspected breach incident to a supervisor or the HIPAA Compliance Officer/EMS Billing Manager.

2. The supervisor and the HIPAA Compliance Officer/EMS Billing Manager will notify management about the suspected incident.
3. The HIPAA Compliance Officer/EMS Billing Manager shall document the date that the suspected breach of unsecured PHI occurred (if known) and the date(s) on which the supervisor and the HIPAA Compliance Officer/EMS Billing Manager were notified about the incident.

### ***Breach Notification to Affected Individuals***

1. Following the discovery of a breach of unsecured PHI, Winchester Fire & Rescue 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 HIPAA Compliance Officer/EMS Billing Manager shall be the party who is primarily responsible to make proper notice, in consultation with Winchester Fire & Rescue management.
2. A breach shall be treated as discovered by Winchester Fire & Rescue as of the first day on which the breach is known, or, by exercising reasonable diligence would have been known to Winchester Fire & Rescue or any person, other than the person committing the breach, who is a staff member or agent of Winchester Fire & Rescue.
3. Winchester Fire & Rescue shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
4. If a law enforcement official states to Winchester Fire & Rescue that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, Winchester Fire & Rescue shall:
  - a. 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
  - b. 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 HIPAA Compliance Officer/EMS Billing Manager shall document the statement, including the identity of the official making the statement.
5. Winchester Fire & Rescue shall 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 agreed to receive electronic notice of breaches, Winchester Fire & Rescue may provide notice by electronic mail. The

notification may be provided in one or more mailings as information becomes available.

6. The HIPAA Compliance Officer/EMS Billing Manager shall utilize Winchester Fire & Rescue's "Individual Notice of Breach of Unsecured PHI" (Attachment B) when sending notice to affected parties. The Notice shall include, to the extent possible:
  - 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 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);
  - c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
  - d. A brief description of what Winchester Fire & Rescue is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
  - e. Contact procedures for individuals to ask questions or learn additional information about the incident from Winchester Fire & Rescue. These contact procedures shall include a toll-free telephone number and an e-mail address to reach Winchester Fire & Rescue's HIPAA Compliance Officer/EMS Billing Manager.
  - f. Contact information to file a complaint to The Office of Civil Rights.
7. If the HIPAA Compliance Officer/EMS Billing Manager determines that affected individuals need to be contacted immediately to protect them from potential harm, the HIPAA Compliance Officer/EMS Billing Manager shall contact those individuals by telephone or other means as soon as possible. Winchester Fire & Rescue shall still send written notice to these individuals about the incident.
8. If Winchester Fire & Rescue knows that any affected individual is deceased and Winchester Fire & Rescue has the address of the next of kin or personal representative of the individual, Winchester Fire & Rescue shall provide written notification by first class mail to either the next of kin or personal representative.
9. If Winchester Fire & Rescue has insufficient or out-of-date contact information for any affected individuals, Winchester Fire & Rescue shall use a substitute form of notice that, in the informed opinion of the HIPAA Compliance Officer/EMS Billing Manager, 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. Substitute notice will be provided in the following manner:

- a. If there is insufficient or out-of-date contact information for fewer than 10 affected individuals, then substitute notice may be provided by an alternative form of written notice such as placing a notice in the newspaper, calling the patient, or other means.
- b. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall: (i) be conspicuously posted on Winchester Fire & Rescue 's home page of its website for 90 days, or conspicuous notice in major print or broadcast media in geographic areas where each affected individual likely resides; and (ii) include a toll-free phone number for Winchester Fire & Rescue that remains active for at least 90 days where individuals can learn whether their unsecured PHI may be included in the breach.

### ***Breach Notification to the Media***

1. For a breach of unsecured PHI involving more than 500 residents of a single state or jurisdiction, Winchester Fire & Rescue shall notify prominent media outlets serving the state or jurisdiction about the breach. The HIPAA Compliance Officer/EMS Billing Manager shall be the party in charge of making such notice and shall make such notification in consultation with Winchester Fire & Rescue management and legal counsel.
2. Notification to the media shall be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.
3. Notification to the media shall include all information that must be included in individual notice.

### ***Breach Notification to HHS***

1. Winchester Fire & Rescue shall notify HHS of all breaches of unsecured PHI in accordance with this policy.
  - a. For breaches of unsecured PHI involving 500 or more individuals, Winchester Fire & Rescue shall 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 HIPAA Compliance Officer/EMS Billing Manager shall be responsible for ensuring that such notice is submitted to HHS and must consult management before submitting the information to HHS.

- b. For breaches of unsecured PHI involving less than 500 individuals, Winchester Fire & Rescue shall maintain a log of such breaches and report them to HHS on an annual basis. The HIPAA Compliance Officer/EMS Billing Manager shall report these breaches to HHS annually, no later than 60 days after the end of the calendar year in which these breaches were discovered. This shall be done in the manner specified on the HHS Website at: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/>. The HIPAA Compliance Officer/EMS Billing Manager shall ensure that the information is submitted to HHS by March 1 of each year and must consult with management before submitting the information to HHS.

### ***Breach Notification in Accordance with State Law***

1. The HIPAA Compliance Officer/EMS Billing Manager shall also determine, in consultation with legal counsel, whether Winchester Fire & Rescue has any additional breach notification obligations under applicable Virginia laws or other state laws.
2. Winchester Fire & Rescue must look to each state in which an affected individual resides when making this determination and shall consult legal counsel licensed to practice in those states.

### ***Administrative Requirements***

1. The HIPAA Compliance Officer/EMS Billing Manager shall record and maintain thorough records of all activities related to suspected and actual breach incidents.
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 management with recommendation from the HIPAA Compliance Officer/EMS Billing Manager. The HIPAA Compliance Officer/EMS Billing Manager shall coordinate communications with outside organizations and law enforcement.
3. Winchester Fire & Rescue will train all members of its staff so that they are able to identify suspected breaches of unsecured PHI and know to report all suspected breaches to the appropriate party immediately.
4. Staff members who violate this policy will be subject to disciplinary action, up to and including termination.

Attachment A



Internal HIPAA  
Breach Form.doc

Attachment B



Breach of PHI  
Notification Letter.do