Jackson Hole Fire/EMS Operations Manual

Approved by: Brady Hansen, Chief

Title: **Breaches of Unsecured PHI**
Division: 17
Article: 5.11
Date: April 2018
Pages: 11

PURPOSE

Under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") Jackson Hole Fire/EMS 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. Jackson Hole Fire/EMS also has an obligation to notify the Department of Health and Human Services ("HHS") of all breaches. In some cases, Jackson Hole Fire/EMS must notify media outlets about breaches of unsecured PHI. This policy details how Jackson Hole Fire/EMS will process and respond to suspected and actual breaches of unsecured PHI.

SECTION I – SCOPE

This Policy applies to all Jackson Hole Fire/EMS members, both employees and volunteers, who come into contact with PHI. All suspected breach incidents shall be brought to the attention of the Jackson Hole Fire/EMS HIPAA Compliance Officer and the HIPAA Compliance Officer shall investigate each incident and initiate the appropriate response to the incident.

SECTION II – BREACH DEFINED

1. A breach is the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

    a. An acquisition, access, use, or disclosure of PHI created, received, maintained or transmitted by Jackson Hole Fire/EMS that is not permitted by HIPAA is presumed to be a breach unless Jackson Hole Fire/EMS demonstrates that there is a low probability that the PHI has been compromised based on a "risk assessment" of the following factors, which include, but are not limited to:

        i. The nature and extent of the PHI breach, including the types of identifiers and the likelihood of re-identification;

        ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and
iv. The extent to which the risk to the PHI has been mitigated.

b. "*Unsecured protected health Information*" is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS for securing PHI - available on HHS's website at: http://www.hhs.gov/ocr/privacy. Generally, PHI is "unsecured" if it is not encrypted by strong encryption technology or if it has not been properly destroyed. If the PHI is able to be used, read, or deciphered it is "unsecured."

2. A breach does not include any of the following:

a. Unintentional acquisition, access, or use of unsecured PHI by a member of Jackson Hole Fire/EMS or someone acting under the authority of Jackson Hole Fire/EMS 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.

b. Any inadvertent disclosure of PHI by a Jackson Hole Fire/EMS member who is generally authorized to access PHI to another member of Jackson Hole Fire/EMS 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.

c. A disclosure of PHI where Jackson Hole Fire/EMS has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

SECTION III – REPORTING A SUSPECTED BREACH INCIDENT

1. All Jackson Hole Fire/EMS members are responsible for immediately reporting a suspected breach incident to a supervisor or the HIPAA Compliance Officer. Jackson Hole Fire/EMS staff members shall report all known and suspected HIPAA violations.

2. The HIPAA Compliance Officer will notify management about the suspected incident.

3. The HIPAA Compliance Officer 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 were notified about the incident.

SECTION IV – INVESTIGATING A SUSPECTED BREACH INCIDENT

1. The HIPAA Compliance Officer shall then initiate an investigation to determine whether an actual breach has occurred and what actions, if any, are necessary.

2. The HIPAA Compliance Officer shall interview all necessary parties who may have information about the incident. The member who reported the suspected incident and other members with

knowledge of the incident should be asked to complete Jackson Hole Fire/EMS's "Internal Breach/Security Incident Reporting Form" (see below). Members should be required to convey all information that they know about the incident and to cooperate in any subsequent investigation regarding the incident.

3. After gathering all available information about the incident, the HIPAA Compliance Officer shall conduct an analysis to determine whether an actual breach of unsecured PHI occurred. Jackson Hole Fire/EMS shall consult with legal counsel whenever necessary in making this determination. The HIPAA Compliance Officer shall utilize Jackson Hole Fire/EMS's Breach Analysis Steps (see below) in making this determination.

4. If the Compliance Officer determines that a breach of unsecured PHI has **not** occurred, the reasons behind that conclusion shall be thoroughly documented.

5. If the HIPAA Compliance Officer determines that a breach of unsecured PHI has occurred, the reasons behind that conclusion shall be thoroughly documented and the HIPAA Compliance Officer shall proceed to notify all necessary parties in accordance with this policy.

SECTION V – BREACH NOTIFICATION TO AFFECTED INDIVUDUALS

1. Following the discovery of a breach of unsecured PHI, Jackson Hole Fire/EMS 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 shall be the party who is primarily responsible to make proper notice, in consultation with Jackson Hole Fire/EMS management.

2. A breach shall be treated as discovered by Jackson Hole Fire/EMS as of the first day on which the breach is known, or, by exercising reasonable diligence would have been known to Jackson Hole Fire/EMS or any person, other than the person committing the breach, who is a staff member or agent of Jackson Hole Fire/EMS.

3. Jackson Hole Fire/EMS 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 Jackson Hole Fire/EMS that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, Jackson Hole Fire/EMS 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 shall document the statement, including the identity of the official making the statement.

5. Jackson Hole Fire/EMS 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, Jackson Hole Fire/EMS 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 shall utilize Jackson Hole Fire/EMS's "Individual Notice of Breach of Unsecured PHI" (see below) 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 Jackson Hole Fire/EMS 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 Jackson Hole Fire/EMS. These contract procedures shall include a toll-free telephone number and an e-mail address to reach Jackson Hole Fire/EMS's HIPAA Compliance Officer.

7. If the HIPAA Compliance Officer determines that affected individuals need to be contacted immediately to protect them from potential harm, the HIPAA Compliance Officer shall contact those individuals by telephone or other means as soon as possible. Jackson Hole Fire/EMS shall still send written notice to these individuals about the incident.

8. If Jackson Hole Fire/EMS knows that any affected individual is deceased and Jackson Hole Fire/EMS has the address of the next of kin or personal representative of the individual, Jackson Hole Fire/EMS shall provide written notification by first class mail to either the next of kin or personal representative.

9. If Jackson Hole Fire/EMS has insufficient or out-of-date contact information for any affected individuals, Jackson Hole Fire/EMS shall use a substitute form of notice that, in the informed opinion of the HIPAA 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. 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 Jackson Hole Fire/EMS'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 Jackson Hole Fire/EMS that remains active for at least 90 days where individuals can learn whether their unsecured PHI may be included in the breach.

SECTION VI – BREACH NOTIFICATION TO THE MEDIA

1. For a breach of unsecured PHI involving more than 500 residents of a single state or jurisdiction, Jackson Hole Fire/EMS shall notify prominent media outlets serving the state or jurisdiction about the breach. The HIPAA Compliance Officer shall be the party in charge of making such notice and shall make such notification in consultation with Jackson Hole Fire/EMS 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.

SECTION VII – BREACH NOTIFICATION TO HHS

1. Jackson Hole Fire/EMS shall notify the U.S. Department of Health and Human Services "HHS" of all breaches of unsecured PHI in accordance with this policy.

   a. For breaches of unsecured PHI involving 500 or more individuals, Jackson Hole Fire/EMS 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 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, Jackson Hole Fire/EMS shall maintain a log of such breaches and report them to HHS on an annual basis. The HIPAA Compliance Officer shall track these breaches on Jackson Hole Fire/EMS's "Log for Tracking Breach Incidents." The HIPAA Compliance Officer 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 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.

SECTION VIII – BREACH NOTIFICATION IN ACCORDANCE WITH STATE LAW

1. The HIPAA Compliance Officer shall also determine, in consultation with legal counsel, whether Jackson Hole Fire/EMS has any additional breach notification obligations under applicable Wyoming laws or other state laws.

2. Jackson Hole Fire/EMS will review the breach as to any other state in which an affected individual resides when making this determination in consultation with legal counsel.

SECTION IX – ADMINISTRATIVE REQUIREMENTS

1. The HIPAA Compliance Officer 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. The HIPAA Compliance Officer shall coordinate communications with outside organizations and law enforcement.

3. Jackson Hole Fire/EMS 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, whether intentionally or unintentionally, will be subject to disciplinary action.

Jackson Hole Fire/EMS HIPAA Compliance Officer Action Plan:

Breach Analysis Steps

Step 1: **Was there an acquisition, access, use or disclosure of PHI that was created, received, maintained, or transmitted by Jackson Hole Fire/EMS?** The HIPAA Compliance Officer shall determine whether PHI was actually involved in the incident, keeping in mind that PHI only includes individually identifiable information that relates to an individual's healthcare or payment for healthcare.	**YES** Go to Step 2	**NO** There has been no breach of unsecured PHI and breach notification is unnecessary.
Step 2: **Was the PHI involved in the incident "unsecured?"** PHI involved in an incident will be considered to be "unsecured" when it is in electronic form and it is not encrypted.	**YES** Go to Step 3	**NO** If the HIPAA Compliance Officer determines that the PHI involved in the incident was secured in accordance with Jackson Hole Fire/EMS's policies on securing hard copy and electronic PHI, then there has been no breach of unsecured PHI and breach notification is unnecessary.
Step 3: **Was there a HIPAA violation?** The HIPAA Compliance Officer must make a determination that there was a violation of the HIPAA Privacy Rule. The incident must involve a use or disclosure that is not permitted by HIPAA.	**YES** Go to Step 4	**NO** There has been no breach of unsecured PHI and breach notification is unnecessary.
Step 4: **Did the incident compromise the security or privacy of the PHI involved?** To determine whether the incident compromised the security or privacy of the PHI that was potentially breached, the HIPAA Compliance Officer must look to the 4-factors outlined below: **Factor** — **Explanation** **1. The nature and extent of the PHI involved** — Consider the type and amount of PHI involved and whether the incident involved sensitive information. For example, credit card numbers, social security numbers, or other information that could be used for identity theft or financial fraud more likely compromises the security of information. The same is true for clinical information, especially detailed clinical information (e.g., treatment, medication, medical history information, etc.).	**Yes** Go to Step 5	**NO** There has been no breach of unsecured PHI and breach notification is unnecessary.

2. The person who used the PHI or to whom the disclosure was made	Consider whether the person who received the information has obligations to protect the information. For example, other covered entities are obligated to protect PHI that they receive in the same manner as Jackson Hole Fire/EMS.		
3. Whether the PHI was actually acquired or viewed	Determine whether the improperly disclosed PHI was returned *before* being accessed for an improper purpose.		
4. The extent to which the risk to the PHI has been mitigated	Consider whether immediate steps were taken to mitigate the potential harm from the improper use or disclosure of the PHI.		
Step Five: Does a breach exception apply? The HIPAA Compliance Officer must also determine whether one of the breach exceptions outlined in the Breach Notification Rule applies to the incident. If so, there is no reportable breach. The three breach exceptions are: • **Unintentional Access, Acquisition or Use of PHI.** The incident involved *unintentional* access, acquisition or use of PHI by a workforce member of Jackson Hole Fire/EMS or someone acting under the authority of Jackson Hole Fire/EMS. The unintentional incident must: (1) be made in good faith; (2) made within the scope of employment; and (3) not result in further improper use or disclosure of PHI. • **Inadvertent Disclosure to an Authorized Party.** Inadvertent disclosure between parties at Jackson Hole Fire/EMS who are authorized to access PHI is not a breach if the PHI is not further used or disclosed in violation of HIPAA. "Authorized to access PHI" means that the two parties involved in the incident are authorized to access PHI *in general* - not necessarily that they are authorized to access the same type of PHI. • **Disclosure Where Retention Was Not Possible.** If the HIPAA Compliance Officer can demonstrate that an unauthorized recipient of the improperly disclosed PHI would not reasonably have been able to retain the PHI, this breach exception applies.	**Yes** Jackson Hole Fire/EMS does not have to make breach notification.	**NO** Jackson Hole Fire/EMS must make breach notification in accordance with Jackson Hole Fire/EMS's "Policy on Breaches of Unsecured Protected Health Information."

Jackson Hole Fire/EMS
Internal Breach/Security Incident Reporting Form

All personnel must report all known and suspected breaches of unsecured PHI and all security incidents immediately to the HIPAA Compliance Officer. If an incident occurs, or is suspected to have occurred, the member with knowledge of the incident must complete this form to the best of his/her knowledge and provide as much detail about the incident as possible. The member will also be required to participate in any subsequent investigation of the incident and to provide additional details as may be needed.

Date of Discovery of Incident: _____ Date of Report: _____

Complete Description of Incident

(Please include date, time, patients affected, parties involved, whether any hardware or devices were involved and any other details):

_____

_____

_____

_____

_____

_____

Your Name and Title: _____

Signature: _____

Individual Notice of Breach of Unsecured PHI

[INSERT DATE]

Via First Class Mail
[INSERT NAME OF AFFECTED INDIVIDUAL]
[INSERT LAST KNOWN ADDRESS FOR AFFECTED INDIVIDUAL]

Re: [Suspected] Breach of Your Protected Health Information

Dear [INSERT NAME OF AFFECTED PARTY]:

Jackson Hole Fire/EMS is committed to patient privacy and we strive to protect the confidentiality of our patients' healthcare information. We take steps to quickly identify and immediately address all known or suspected breaches of your healthcare information.

Jackson Hole Fire/EMS [believes] [has information] that your health information [may have been] [was] improperly [accessed, used, disclosed]. Therefore, we are providing this notice to you so that you are aware of and informed about the incident, and so that you can take any further steps that may be necessary to protect your health information.

[Provide a brief description of what happened, including the date of the breach and the date Jackson Hole Fire/EMS discovered the breach. *Example:* It was brought to our attention that on April 3, 2014 one of our employees accessed your electronic patient file for non business-related reasons and without authorization. We discovered this on April 5, 2014.]

[Give a brief, generic description of the types of unsecured PHI that were involved in the incident such as: full name, SSN, DOB, home address, account number, condition, etc. *Example:* The file that was breached contained your home address, your Medicare identification number, your healthcare condition, and your date of birth.]

[Explain any steps that the individual should take to protect themselves from potential harm from the breach. *Example:* We recommend that you carefully monitor explanations of benefits (EOBs) or other remittance advice or account statements received from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or bill for health care services that you believe you did not receive, immediately contact your insurer and the health care provider who furnished the services.]

[Briefly explain what Jackson Hole Fire/EMS is doing or has done to investigate the breach, to mitigate harm to the individual, and to protect against further breaches. *Example:* Jackson Hole Fire/EMS has spoken with the employee to ascertain what information was accessed and retained while viewing your file. We also audited access and download logs for that computer to determine whether other unauthorized parties could have gained access to your information and whether any patient information was extracted from the computer. We found no activity that indicates that any other party accessed your information.]

[Provide contact procedures for the individual to ask questions or learn additional information, including either: a toll-free telephone number, an email address, website, or postal address. *Example:* We encourage you to contact us at 307-733-4732 and ask to speak with our HIPAA Compliance Officer, [insert name], for more information about this incident. We are happy to answer your questions or to provide you with any additional information that you might require.]

We sincerely regret any inconvenience that this incident has caused and we have taken all appropriate steps to ensure that your health information is protected and that a similar incident does not happen in the future. We value your trust in Jackson Hole Fire/EMS and we consider patient privacy a top priority. If there is anything we can do to assist you, please contact us at the toll-free number above.

Sincerely,

[Insert name]
HIPAA Compliance Officer
Jackson Hole Fire/EMS