

Verde Valley Ambulance Company Policy on Breaches of Unsecured Protected Health Information

Purpose

Under the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) and the regulations at 45 C.F.R. Part 164, Subpart D, ABC Ambulance 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. Verde Valley Ambulance Company also has an obligation to notify the Department of Health and Human Services (“HHS”) of all breaches. In some cases, Verde Valley Fire District 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.

Scope

This Policy applies to all Verde Valley Ambulance Company staff members who come into contact with PHI. All suspected breach incidents shall be brought to the attention of the HIPAA Compliance Officer, and the HIPAA Compliance Officer shall investigate the incident and initiate the appropriate response to the incident.

Procedure

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. *“Compromises the security or privacy of the protected health information”* means that the incident poses a significant risk of financial, reputational, or other harm to the individual.
 - 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 been improperly destroyed. If the PHI is able to be used, read, or deciphered it is generally “unsecured.”

Examples of Potential Breaches:

- A Verde Valley Ambulance laptop, which contains the PHI of patients of Verde Valley Ambulance Company, is lost or stolen and the data on the laptop could be accessed by an unauthorized party.
- A PCR containing health information of a patient of Verde Valley Ambulance Company is lost or misplaced and there is reason to believe the information could be viewed by an unauthorized party.
- A staff member of Verde Valley Ambulance Company accesses the electronic record of her neighbor in order to snoop on the neighbor's medical history.

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

- a. Unintentional acquisition, access, or use of unsecured PHI by a staff member at Verde Valley Ambulance Company or someone acting under the authority of Verde Valley Ambulance Company 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.

Example: A staff member of Verde Valley Ambulance Company inadvertently picks up the wrong PCR and, after looking at it and realizing the mistake, replaces the PCR in a secure location without further disclosing any information.

- b. Any inadvertent disclosure of PHI by an Verde Valley Ambulance Company staff member who is generally authorized to access PHI to another person at Verde Valley Ambulance Company 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.

Example: A field staff member of Verde Valley Ambulance Company inadvertently furnishes the wrong PCR to a billing staff member at Verde Valley Ambulance Company in order to submit the trip for reimbursement. The billing staff member notifies the field staff member of the mistake and the information is not further used or disclosed.

- c. A disclosure of PHI where Verde Valley Ambulance Company 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.

Example: A bill that was sent to the wrong address is returned, unopened with a stamped statement reading: "Return to Sender."

Reporting a Suspected Breach Incident

1. All Verde Valley Ambulance Company staff members are responsible for immediately reporting a suspected breach incident to a supervisor.
2. The supervisor shall immediately notify the HIPAA Compliance Officer about the incident and convey all information that is known about the incident to the HIPAA Compliance Officer.
3. The HIPAA Compliance Officer will notify management about the suspected incident.
4. 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.

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. The HIPAA Compliance Officer will involve legal counsel in making these determinations whenever possible.
2. The HIPAA Compliance Officer shall interview all necessary parties who may have information about the incident. The staff member who reported the suspected incident and other members with knowledge of the incident should be asked to complete the attached "Security/Breach Incident Form." Staff 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. Verde Valley Ambulance Company shall consult with legal counsel whenever possible in making this determination. The HIPAA Compliance Officer shall also utilize the attached "Breach Analysis Steps for Covered Entities and Business Associates" 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.

Breach Notification to Affected Individuals

1. Following the discovery of a breach of unsecured PHI, Verde Valley Ambulance Company 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 Verde Valley Ambulance management.
2. A breach shall be treated as discovered by Verde Valley Ambulance Company as of the first day on which the breach is known, or, by exercising reasonable diligence would have been known to Verde Valley Ambulance Company or its agents.
3. Verde Valley Ambulance Company 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 Verde Valley Ambulance Company that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, Verde Valley Ambulance Company 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. Verde Valley Ambulance Company 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 agrees to electronic notice and such agreement has not been withdrawn, the Verde Valley

Ambulance Company 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 Verde Valley Ambulance Company's attached Notice to Affected Individuals as a guide 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 Verde Valley Ambulance Company 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, which shall include a toll-free telephone number, an e-mail address, website, or postal address.
7. In any case deemed by Verde Valley Ambulance Company to require urgency because of possible imminent misuse of unsecured PHI, Verde Valley Ambulance Company may provide information to individuals by telephone or other means in addition to written notice.
8. If Verde Valley Ambulance Company knows the individual is deceased and has the address of the next of kin or personal representative of the individual, ABC Ambulance shall provide written notification by first class mail to either the next of kin or personal representative. The notification may be provided in one or more mailings as information becomes available.
9. If Verde Valley Ambulance Company has insufficient or out-of-date contact information that precludes written notification to the individual, Verde Valley Ambulance Company shall use a substitute form of notice reasonably calculated to reach the individual in accordance with this policy. 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.

- a. 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.
- b. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall: (i) be in the form of either a conspicuous posting for 90 days on Verde Valley Ambulance Company 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 toll-free phone number for Verde Valley Ambulance Company 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, Verde Valley Fire District 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 Verde Valley Ambulance Company 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. For breaches of unsecured PHI involving 500 or more individuals, Verde Valley Ambulance Company 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 with legal counsel and management before submitting the information to HHS.
2. For breaches of unsecured PHI involving less than 500 individuals, Verde Valley Ambulance Company shall maintain a log of such breaches. The HIPAA Compliance Officer shall track these breaches on Verde Valley Ambulance Company's "Log for Tracking Breach Incidents." Verde Valley Ambulance Company shall provide information regarding such breaches to HHS annually, no later than 60 days after the end of the calendar year. 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 be responsible for ensuring that the information is submitted to HHS by March 1 of each year and must consult with legal counsel and management before submitting the information to HHS.

Breach Notification in Accordance with State Law

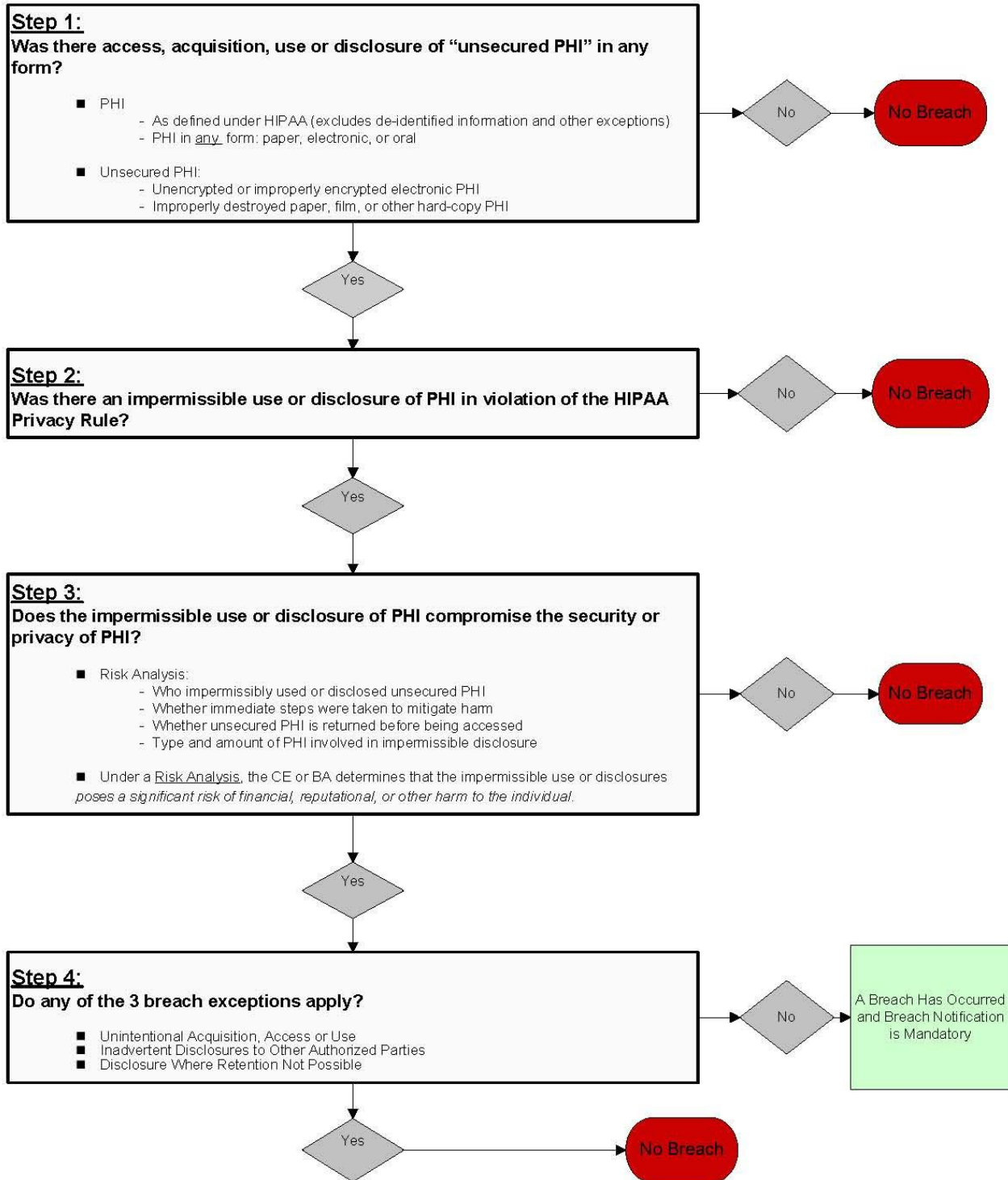
1. The HIPAA Compliance Officer shall also determine, in consultation with legal counsel, whether Verde Valley Ambulance Company has any additional breach notification obligations under applicable state law.
2. Verde Valley Ambulance Company must look to each state in which an affected individual resides when making this determination and shall consult legal counsel licensed to practice in those states.

Administrative Requirements

1. Verde Valley Ambulance Company shall record and maintain thorough records of all activities related to suspected and actual breach incidents. The HIPAA Compliance Officer shall be primarily responsible for documentation of these activities.
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 is responsible for coordinating communications with outside organizations and law enforcement.
3. Verde Valley Ambulance Company 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.



Breach Analysis Steps for Covered Entities and Business Associates





Verde Valley Ambulance Company
P.O. Box 1477, COTTONWOOD, AZ 86326
PHONE: (928) 634-7750 FAX: (928) 634-0719

Security/Breach Incident Reporting Form

All personnel must report all known and suspected security incidents and breaches of unsecured PHI immediately to the HIPAA Compliance Officer. If an incident occurs, or is suspected to have occurred, the staff 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 staff member will also be expected to participate in any subsequent investigation of the incident and to provide additional details as they become available.

Date of Incident:	Date of Report:
Complete Description of Incident: _____ _____ _____ _____ _____ _____	
Identify Specific Individuals Whose PHI May Have Been Breached: _____ _____	
Identify or Describe any Hardware or Software Involved: _____ _____	
Names of Others Involved in the Incident: _____ _____	
<i>Your Name and Title:</i> _____ <i>Signature:</i> _____	

[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]:

Verde Valley Ambulance Company 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 protected healthcare information.

Verde Valley Ambulance Company [believes] [has information that] 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.

[Give a brief description of what happened, including the date of the breach and the date Verde Valley Ambulance Company discovered the breach.

Example: It was brought to our attention that on April 3, 2011 one of our employees accessed your electronic patient file for non business-related reasons and without authorization. We discovered this on April 5, 2011.]

[Give a brief description of the generic types of unsecured PHI that were involved in the breach 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 you believe you did not receive, immediately contact your insurer and the health care provider who furnished the services.]

We also recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you and verify your identity before they open any new accounts or change existing accounts. Please contact one of the three major credit bureaus. Once a credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The numbers for the credit bureaus are:

Equifax: 1-800-685-1111
Experian: 1-888-397-3742
TransUnionCorp: 1-800-680-7289

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, immediately notify the credit bureaus. If you believe an unauthorized account has been opened in your name, immediately contact the financial institution that holds the account.]

[Briefly explain what Verde Valley Ambulance Company is doing or has done to investigate the breach, to mitigate harm to the individual, and to protect against further breaches. *Example:* Verde Valley Ambulance Company 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.]

[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 1-800-555-5555 and ask to speak with our HIPAA Compliance Officer, 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. We assure you that we have taken all appropriate steps to ensure your PHI is protected and that such an incident does not happen in the future. We value your trust in Verde Valley Fire District 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,

[Compliance Officer Name and Address]