HIPAA Breach Notification

June 28, 2010
Policy A-IC-27 **Revised June 13, 2019**

Purpose: To ensure all staff are compliant with the Breach Notifications requirements as set out in 45 CFR §164.400-414.

Policy: It is the policy of Three Rivers District Health Department to comply with all notification requirements as set out in the code of federal regulations as it pertains to Notices in the event of a breach of unsecured protected health information.

Procedure: All employees are subject to and required to comply and be familiar with the breach notifications requirements and procedures as identified below:

I. BREACH NOTIFICATION.
   A. Generally. [45 CFR §164.404(a)(1)] Following discovery of a breach of unsecured protected health information, THREE RIVERS DISTRICT HEALTH DEPARTMENT's Privacy Officer shall notify each individual whose unsecured protected health information has been, or reasonably believed by the Privacy Officer to have been, accessed, acquired, used, or disclosed as a result of that breach. Such notification shall be as stated in this Breach Notification Policy.
   B. When a Breach is Considered to be "Discovered." [45 CFR §164.404(a)(2)] A breach shall be considered to be "discovered" as of the first day on which the breach is known to THREE RIVERS DISTRICT HEALTH DEPARTMENT, or, by exercising reasonable diligence would have been known to THREE RIVERS DISTRICT HEALTH DEPARTMENT. THREE RIVERS DISTRICT HEALTH DEPARTMENT shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of THREE RIVERS DISTRICT HEALTH DEPARTMENT.
   C. Time of Notification. [45 CFR §164.404(b)] The notification to affected individuals shall be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.
   D. Content of Notification. [45 CFR §164.404(c)] The notification to affected individuals shall be written in plain language and include to the extent possible:
      1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. 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, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what THREE RIVERS DISTRICT HEALTH DEPARTMENT is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,
5. Contract procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, Web site, or postal address.
6. Generally, the notice should avoid including any sensitive material, such as the individual's actual social security number or credit card number.

E. As appropriate for the individuals to whom notice is given, reasonable steps shall be taken to have the notification translated into languages that are frequently encountered by THREE RIVERS DISTRICT HEALTH DEPARTMENT and as may be necessary to ensure effective communication with individuals with disabilities.

F. Methods of Notification. [45 CFR §164.404(d)]
   1. Written Notice. The notification to affected individuals shall be by first class mail to the individual at the last known address of the individual, or, if the individual has agreed to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. If THREE RIVERS DISTRICT HEALTH DEPARTMENT knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification may be by first class mail to either the next of kin or the personal representative is permitted. It may be provided in one or more mailings as information is available.
   2. Substitute Notice.
      a. Generally. If there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice, which is reasonably calculated to reach the individual, must be used. However, substitute notice is not required if the insufficient or out-of-date contact information precludes written notice to the next of kin or personal representative.
      b. If Fewer Than 10 Individuals. If there are fewer than 10 individuals to receive substitute notice, the substitute notice may be provided by an alternate form of written notice, telephone, or other means.
      c. If 10 or More Individuals. If there are 10 or more individuals to receive substitute notice, then the substitute notice must:
         (1). Be in the form of either: (A) a conspicuous posting for a period of 90 days on the home page of the Web site of

THREE RIVERS DISTRICT HEALTH DEPARTMENT; or, (B) a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and,

(2). Include a toll-free telephone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

(3). Additional Notice in Urgent Situations. If the Privacy Officer deems the situation to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice stated above.

G. Notification to the Media. [45 CFR §164.406] If a breach of unsecured protected health information involves more than 500 residents of a State or other jurisdiction, THREE RIVERS DISTRICT HEALTH DEPARTMENT shall notify prominent media outlets serving that State or jurisdiction of the breach. This notice will be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. To the extent possible, the notification shall meet the requirements stated in paragraph I.D, "Content of Notification," above, for its content.

H. Notification to the Secretary of HHS. [45 CFR §164.408] Following discovery of a breach, the Privacy Officer shall notify the Secretary of HHS as stated below.

1. Breaches involving 500 or more individuals. If the breach involves 500 or more individuals, with one exception, THREE RIVERS DISTRICT HEALTH DEPARTMENT will provide the Secretary of HHS with notice of the breach contemporaneously with its notice to the affected individuals. The notice will include the same information that is provided to affected individuals and will be provided to the Secretary of HHS in the manner specified on the HHS Web site. The exception is when there is a law enforcement delay (see, paragraph I.J, below).
2. Breaches involving less than 500 individuals. If the breach involves less than 500 individuals, the Privacy Officer will maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the Secretary of HHS with notice of breaches occurring during the preceding calendar year. (For 2009, the information to be submitted will be only for breaches, if any, occurring on or after September 23, 2009.) This log will be kept for six years.

I. Notification from a Business Associate. [45 CFR §164.410] When notification is received from a business associate of THREE RIVERS DISTRICT HEALTH DEPARTMENT of its discovery of a breach of unsecured protected health information, the Privacy Officer shall give notice to affected individuals in accordance with this Breach Notification Policy. Provided, however, if the agreement between THREE RIVERS DISTRICT HEALTH DEPARTMENT and the business associate permits, the Privacy Officer may require the business associate to give such notice.

J. Law Enforcement Delay. [45 CFR §164.412] Notwithstanding anything in this Breach Notification Policy to the contrary, if a law enforcement official states to THREE RIVERS DISTRICT HEALTH DEPARTMENT that a notification, notice, or posting required by this Breach Notification Policy would impede a criminal investigation or cause damage to national security, the Privacy Officer shall:
    1. If the statement of the law enforcement official is in writing and specifies how long of a delay is required, delay the notification, notice, or posting for the time period specified in the writing; or,
    2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily but no longer than 30 days from the date of the statement, unless a written statement as described in subparagraph 1, above, is submitted during that time.
    3. Any member of the workforce of THREE RIVERS DISTRICT HEALTH DEPARTMENT who is contacted by a law enforcement official in this regard shall immediately refer him/her to the Privacy Officer.

II. ADMINISTRATIVE POLICIES.

A. Training. [45 CFR §164.530(b)] All members of THREE RIVERS DISTRICT HEALTH DEPARTMENT's workforce shall be trained annually on THREE RIVERS DISTRICT HEALTH DEPARTMENT's breach notification policy and procedures as necessary and appropriate for the members of the workforce to carry out their functions within THREE RIVERS DISTRICT HEALTH DEPARTMENT.
    1. Each member of the workforce on September 23, 2009 shall be trained on the TRD breach notification policy. Thereafter, each new member of the workforce shall be trained within 60 calendar days after the person joins the workforce. Each member of the workforce whose functions are affected by a material change in these privacy policies or procedures shall be trained at the next quarterly staff meeting after the material change becomes effective.
    2. Documentation of the training for each member of the workforce shall be kept in written or electronic form for six (6) years after the date of its creation or the date that persons ceases to be a member of THREE RIVERS DISTRICT HEALTH DEPARTMENT's workforce, which is later.

B. Complaints. [45 CFR §164.530(d)(1)] THREE RIVERS DISTRICT HEALTH DEPARTMENT's Privacy Officer shall be responsible for receiving complaints concerning THREE RIVERS DISTRICT HEALTH DEPARTMENT's breach notification policies and procedures and compliance with that policy and those procedures.

C. Sanctions. [45 CFR §164.530(e)(1)] Any member of THREE RIVERS DISTRICT HEALTH DEPARTMENT's workforce who fails to comply with THREE RIVERS DISTRICT HEALTH DEPARTMENT's Breach Notification Policy or the requirements of the HIPAA Breach Notification Rule shall be

subject to sanctions imposed through THREE RIVERS DISTRICT HEALTH DEPARTMENT's discipline and discharge policies up to and including termination. Examples of certain actions that may require sanctions are:

1. Inadvertent failure to promptly report any breach of unsecured private health information to the Privacy Officer.
2. Knowing failure to promptly report any breach of unsecured private health information to the Privacy Officer.
3. Inadvertent violation of any part of THREE RIVERS DISTRICT HEALTH DEPARTMENT's Breach Notification Policy or requirement of the HIPAA Breach Notification Rule.
4. Knowing violation of any part of THREE RIVERS DISTRICT HEALTH DEPARTMENT's Breach Notification Policy or requirement of the HIPAA Breach Notification Rule.
5. The *Personnel Specialist* shall cause written documentation of the sanctions that are applied, if any, to be kept in written or electronic form for six (6) years after the date of its creation or the date when it is last in effect, whichever is later. *[45 CFR §164.530(e)(2)]*

D. Prohibition on Intimidating or Retaliatory Acts. [45 CFR §164.530(g)] Neither THREE RIVERS DISTRICT HEALTH DEPARTMENT nor any member of THREE RIVERS DISTRICT HEALTH DEPARTMENT's workforce may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by, this Breach Notification Rule, including filing a complaint under this Rule.

E. Prohibition on Waiver of Rights. [45 CFR §164.530(h)] No member of THREE RIVERS DISTRICT HEALTH DEPARTMENT's workforce may require an individual to waive the individual's rights under this Breach Notification Rule as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

F. Changes to Policies and Procedures. [45 CFR §164.530(i)(1)] The Privacy Officer shall promptly change this Breach Notification Policy as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Breach Notification Rule.

G. Documentation. [45 CFR §164.530(j)] The Privacy Officer shall take, or cause to be taken, each of the following actions:

1. Maintain THREE RIVERS DISTRICT HEALTH DEPARTMENT's breach notification policies and procedures in written or electronic form;
2. If a communication is required by THREE RIVERS DISTRICT HEALTH DEPARTMENT's Breach notification policies and procedures, or by the HIPAA Breach Notification Rule, to be in writing, maintain that writing, or an electronic copy, as documentation;
3. If an action, activity, or designation is required by THREE RIVERS DISTRICT HEALTH DEPARTMENT's breach notification policies and procedures, or by the HIPAA Breach Notification Rule, to be documented, maintain a written or electronic record of that action, activity or designation.

4. Maintain documentation sufficient to meet THREE RIVERS DISTRICT HEALTH DEPARTMENT's burden of demonstrating that all notifications were made as required by this Breach Notification Policy or that a use or disclosure did not constitute a breach. [45 CFR §164.414(b)]

H. Period of Retention. *[45 CFR §164.530(j)(2)]* Documentation required by paragraph II.G, "Documentation", above, shall be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

I. Security Risk Assessment, Form A-IC-27 (A). The Privacy Officer shall conduct a risk assessment upon identification or discovery of a breach utilizing the standards set out in the final rule March 26, 2013 to determine notice requirements prior to providing notice(s). The assessment shall at minimum:
   1. Determine the nature of the PHI involved, including the types of identifiers and likelihood of re-identification;
   2. Identify the unauthorized person who used the PHI or to whom the PHI was disclosed;
   3. Confirm whether the PHI was actually acquired or viewed; and
   4. Determine the extent to which the risk to the PHI has been mitigated.

III. DEFINITIONS. As used in this Breach Notification Policy, the following terms and phrases shall have the following meanings.

A. Breach. [45 CFR §164.402] "Breach" means the acquisition, access, use or disclosure of protected health information in a manner not permitted by the Federal HIPAA Privacy Rule which compromises the security or privacy of the protected health information. Provided, however, breach does not include:
   1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of THREE RIVERS DISTRICT HEALTH DEPARTMENT or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Federal HIPAA Privacy Rule.
   2. Any inadvertent disclosure by a person who is authorized to access protected health information at THREE RIVERS DISTRICT HEALTH DEPARTMENT or business associate to another person authorized to access protected health information at THREE RIVERS DISTRICT HEALTH DEPARTMENT or the same business associate, or organized health care arrangement in which THREE RIVERS DISTRICT HEALTH DEPARTMENT participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Federal HIPAA Privacy Rule.
   3. A disclosure of protected health information where THREE RIVERS DISTRICT HEALTH DEPARTMENT or a 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.

B. Presumed Breach – is the acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR §164.500-534 unless the covered entity or business associate, as applicable, demonstrates that there is a

low probability that the protected health information has been compromised based on a risk assessment of at least 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 actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

C. Unsecured protected health information. [45 CFR §164.402] "Unsecured protected health information" means protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services (the "Secretary of HHS") through guidance issued by the Secretary of HHS on the HHS Web site.

District Director **Date**

Chairperson, Three Rivers District Board of Health **Date**

FORM A-IC-27(A) **Three Rivers District Health Department**

Breach Notification Risk Assessment Tool

Incident/File/Name	Event Date: Discovery Date:
Number of Individuals Affected	
Point of Contact	Phone#
Brief Summary/Findings	Final Decision

Source of Incident: Who was responsible for the inappropriate acquisition, access, use or disclosure (incident)? Circle your answer…. If a Business Associate or subcontractor is the source of the incident, enter the date of the Business Associate or their Business Associate made you aware of incident.	☐ Internal to the Agency or, ☐ Business Associate Date:
Is there a BAA or other agreement in place?	☐ Yes ☐ No
Have they performed a breach assessment of their own?	☐ Yes ☐ No
Have any notifications been made by the BA or subcontractor?	☐ Yes ☐ No
Are you the Business Associate or subcontractor? When was it discovered or when should it have been discovered?	☐ Yes ☐ No Date:
If you are the Business Associate or subcontractor, enter the date you notified the other Covered Entity of the incident.	Date:
Enter the date that our organization became aware of the incident.	Date:

Section 164.410(a)(2) further provides that a covered entity is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

--- Section 1 --- **TRDHD Breach Notification Risk Assessment Tool**	
1. Is there a HIPAA Privacy or Security Rule violation involving the acquisition, access, use or disclosure of PHI? ***If No, then STOP here. No breach has occurred.*** *If Yes, then proceed to the next question.*	☐ Yes ☐ No
2. Was data secured or properly destroyed in compliance with the requirements which state only encryption and destruction, consistent with National Institute of Standards and Technology (NIST) guidelines 13402(h)(2) under public law 111-5, renders protected health information unusable, unreadable, or indecipherable to "unauthorized persons." ***If No, then STOP here. No breach has occurred.*** *If Yes, then proceed to the next question.*	☐ Yes ☐ No
3. Does this incident qualify under one of the following exceptions? ***If Yes, then STOP here. No breach has occurred that requires notification.*** *If No, then proceed to the next question to work through the assessment.*	☐ Yes ☐ No
An unintentional acquisition, access, or use of PHI by a workforce member is such acquisition, access, or use was made in good faith and within the scope of the workforce member's authority and does not result in further use or disclosure not permitted by the privacy rules. (45 C.F.R. § 164.402). For example, no notification is required where an employee mistakenly looks at the wrong patient's PHI but does not further use or disclose the PHI.	
An 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, and the PHI is not further used or disclosed in a manner not permitted by the privacy rules. (*Id*.). For example, no notification is required if a medical staff member mistakenly discloses PHI to the wrong nurse at a facility but the nurse does not further use or disclose the PHI improperly.	
A disclosure where the person making the disclosure has a good faith belief that the unauthorized recipient would not reasonably be able to retain the PHI. (*Id*.). For example, no notification is required if a nurse mistakenly hands PHI to the wrong patient but immediately retrieves the information before the recipient has a chance to read it.	

If you did not hit a STOP in Section 1, continue through the remainder of the assessment to determine whether there is a low probability that the PHI has been compromised.

Go to Section 2

<table>
<tr><th colspan="5">--- Section 2 ---
TRDHD Breach Notification Risk Assessment Tool</th></tr>
<tr><td>Risk Assessment Factors</td><td colspan="4">Circumstances of the Incident
Circle each</td></tr>
<tr><td></td><td colspan="3">Considerations Elements</td><td>Score</td></tr>
<tr><td rowspan="2">1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

For example, if a file or known abuse victim is breached that includes the victims' addresses, then you will probably want to rank the breach of this data as a high probability of causing harm to the person(s) affected by the breach. However, under other circumstances just the release of an address may be considered low risk of harm to the person(s) impacted by the breach. [1]</td><td></td><td><u>Clinical Information</u>

• Name
• MRN
• Address
• Room#
• Email
• DOB
• Provider
• Date of Service
• Limited Data Set
• Non-Diagnostic Information
• Other</td><td rowspan="2">Consider the risk of re-identification</td><td>Low Probability</td></tr>
<tr><td></td><td>• SSN
• Sensitive Diagnosis Info
• Sensitive PHI which may include info about sensitive diagnosis, such as HIV, Substance Abuse, and/or Mental Health
• STD
• Medications that indicate sensitive diagnosis
• Other</td><td>Probability</td></tr>
</table>

[1] All examples cited are from the narrative in the Final Rule

--- Section 2 --- TRDHD Breach Notification Risk Assessment Tool			
Risk Assessment Factors	Circumstances of the Incident Circle each		
	Considerations Elements		Score
2. The unauthorized person who used the PHI or to whom disclosure was made. If the information impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the protected health information has the ability to re-identify the information. For example, if information containing dates of health care service and diagnosis of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the PHI has been compromised. (78 F.R. 5643). Does the recipient have confidentiality obligations? (5643)		• Your Business Associate • Another Covered Entity • Internal Workforce • Wrong Payor (not the patient's) • Unauthorized family member • Other	Low Probability
		• Non-covered Entity • Media • Unknown/Lost/ Stolen • Member of the general public • Patient employer • Other	Probability
3. Whether the PHI was actually acquired or viewed. For example, there is likely a low risk if a misdirected letter is returned unopened or a lost computer is recovered and it is confirmed that PHI was not accessed. Conversely, there is a higher risk where the recipient opens and reads a misdirected letter even though she reports the letter to the covered entity.		• Unauthorized internal acquisition, access and/or use without disclosure outside of organization Extent to which PHI was in fact accessed (5643) • Verbal disclosure • View only • Other	Low Probability
		• Paper/Fax • Electronic • Other	Probability

--- Section 2 --- TRDHD Breach Notification Risk Assessment Tool			
Risk Assessment Factors	Circumstances of the Incident Circle each		
	Considerations Elements		
4. Whether the risk to the PHI has been mitigated. For example, there may be a lower risk if a fax is directed to the wrong number, but the recipient confirms that they returned or destroyed the PHI; the PHI has not been and will not be further used or disclosed; and the recipient is reliable. (Id.). This factor highlights the need for covered entities and business associates to immediately identify and respond to potential breaches to reduce the probability that PHI is compromised and the necessity of breach reporting.	Disposition (What happened to the information after the initial disclosure) Has the risk to PHI been mitigated? Did we get it back? Certification/ attestation of destruction? Reliability of attestation? Unreadable/ undecipherable? Other impact? Controls in place to influence ability to compromise? Flag records Like red flags? Value of Data? (insurance number vs other types)	• Visual, viewed only with no further disclosure or retention • Obtained reliable assurances that the use or disclosure was very limited • Obtained reliable assurances that the PHI will not be further used or disclosed? • Information returned complete • Information properly destroyed and attested to • Information properly destroyed (unattested) • Electronically Deleted (unsure of backup status) • Other	

--- Section 2 --- TRDHD Breach Notification Risk Assessment Tool		
5. Other Factors	• Electronic Data wiped • Information/Device Encrypted, but does not meet compliance with NIST Standards • Hardcopy or electronic media destroyed, but does not meet compliance with NIST Standards • Encrypted – Encryption keys not secured • Password Protected • No Controls Safeguards listed in the DHHS Breach Reporting Form: • Firewalls, Packet Filtering (router-based) • Secure Browser Sessions • Strong Authentication • Encrypted Wireless, Physical Security • Logical Access Control • Anti-virus software, Intrusion Detection • Biometrics • Other	

Additional information considered in your determination:

Analysis Points/Narrative
Ensure Mitigation or Process Correction within 30 days for reoccurrence

SCORING

If the risk assessment demonstrates a low probability that the PHI has been compromised, the analysis should be documented without notification. If the risk assessment fails to demonstrate a low probability that the PHI has been compromised, the breach is required to be reported unless one of the regulatory exceptions applies.

The scoring is meant to serve only as a guide in decision making and not designed to make the notification decision. There are a variety of factors and mitigations that may be involved in the incident that this tool may not foresee or predict. This assessment tool was developed as a way to assist in documenting the actions, considering risk factors and circumstances and aiding in a final decision of making a breach notification or not making a breach notification. There is no "scoring" element for factors #4 and #5 as they were considered mitigation factors as opposed to risk factors.

The risk factors carry a possible outcome of "Low Probability" or "Probability."

Probability of Compromised Information

Low Probability **High Probability**

Notification Unlikely — Articulate and Document Decision To Notify or Not — Notification Likely

Breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.