STATE OF UTAH DEPARTMENT OF HEALTH	Number: 14.00	Page 1 of 5
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: HITECH Breach Policies	Subject: Data Breach – Protected Health Information	

Effective Date: October 9, 2012

1. Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the Utah Department of Health covered functions (DEPARTMENT), or, by exercising reasonable diligence would have been, known to DEPARTMENT (includes breaches by DEPARTMENT's business associates). DEPARTMENT shall be 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 (business associate) of DEPARTMENT. Following the discovery of a potential breach, DEPARTMENT shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by DEPARTMENT to have been, accessed, acquired, used, or disclosed as a result of the breach. DEPARTMENT shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. Breach Investigation: DEPARTMENT shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in DEPARTMENT as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

3. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, DEPARTMENT will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. DEPARTMENT shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. DEPARTMENT has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, DEPARTMENT will determine the need to move forward with breach notification.

4. Timeliness of Notification: Upon determination that breach notification is required, the notice shall

be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by DEPARTMENT involved or the business associate involved. It is the responsibility of DEPARTMENT to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to DEPARTMENT that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, DEPARTMENT shall:
   A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
   B. 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 and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:
   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 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).
   C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
   D. A brief description of what DEPARTMENT is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
   E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

7. Methods of Notification: The method of notification will depend on the individuals/ entities to be notified. The following methods must be utilized accordingly:
   A. Notice to Individual(s): Notice shall be provided promptly and in the following form:
      1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If DEPARTMENT knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.
      2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

         a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of DEPARTMENT's website, or a conspicuous notice in a major print or broadcast media in DEPARTMENT's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

8. If DEPARTMENT determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.
   A. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.
   B. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.
      1. For breaches involving 500 or more individuals, DEPARTMENT shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
      2. For breaches involving less than 500 individuals, DEPARTMENT will maintain a log of the breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

9. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, DEPARTMENT shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected.

10. Business Associate Responsibilities: The business associate (BA) of DEPARTMENT that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify DEPARTMENT of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide DEPARTMENT with any other available information that DEPARTMENT is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, DEPARTMENT will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

11. Workforce Training: DEPARTMENT shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within DEPARTMENT.

12. Complaints: DEPARTMENT must provide a process for individuals to make complaints concerning DEPARTMENT's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about DEPARTMENT's breach notification processes.

13. Sanctions: DEPARTMENT shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

14. Retaliation/Waiver: DEPARTMENT may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. DEPARTMENT may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 14.01	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: HITECH Breach Policies	Subject: Data Breach Discovery	

Effective Date: October 9, 2012

Policy:
DEPARTMENT will employ policies, technologies, and education to identify security breaches.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 14.02	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: HITECH Breach Policies	Subject: Data Breach Management	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure that if a data breach is discovered, the steps laid out in this policy will be followed in order to prevent further damage, assess the severity of the breach, and manage all breach-related activities.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 14.03	Page 1 of 1
	Original Issue Date: 10/09/201	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: HITECH Breach Policies	Subject: Data Breach Notification	

Effective Date: October 9, 2012

Policy:
DEPARTMENT will notify persons and organization that have been impacted by a data breach.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 14.04	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: HITECH Breach Policies	Subject: Data Breach Notification to HHS	

Effective Date: October 9, 2012

Policy:
DEPARTMENT will notify persons and organizations that have been impacted by a data breach, and require notification as determined by Policy #14.03, Data Breach Notification Policy. This policy will serve as guidance to determine if, when and how HHS is to be notified.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 14.05	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: HITECH Breach Policies	Subject: Data Breach Notification to Individual	

Effective Date: October 9, 2012

Policy:
DEPARTMENT will notify persons that have been impacted by a data breach in accordance with Policy #14.03, Data Breach Notification Policy.

This policy will assist in determining if, when and how impacted individuals are to be notified.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 14.06	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: HITECH Breach Policies	Subject: Data Breach Notification to Media	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will notify persons that have been impacted by a data breach in accordance with Policy #14.03, Data Breach Notification Policy. This policy will provide guidance to determine if, when and how the media is to be notified.