STATE OF VERMONT Agency of Human Services (AHS)		VERMONT AGENCY OF HUMAN SERVICES
HIPAA Breach Notification	**REVISION HISTORY:**	**Chapter/Number**
	EFFECTIVE DATE:	Attachments / Related Documents:
Authorizing Signature: AL / Gobeille Al Gobeille, Secretary, Agency of Human Services		Date Signed: 7.5.17

PURPOSE/POLICY STATEMENT:

To notify and protect individuals whose protected health information (PHI) is breached, as that term is defined below. When a member of the Agency of Human Services (AHS) workforce impermissibly uses or discloses an individual's PHI, AHS will promptly notify the affected individual(s) so that they are aware of the breach and have the opportunity to take steps to protect themselves from the consequences of it. AHS will not provide notice when it determines that there is a low probability that the PHI was compromised.

BACKGROUND and REFERENCES:

On August 19, 2009, the United States Department of Health and Human Services (HHS) issued regulations requiring Covered Entities, such as AHS, to notify individuals when their health information is improperly acquired, accessed, used or disclosed under the Health Insurance Portability and Accountability Act (HIPAA). The regulations defined the term breach for the first time and added a requirement that Covered Entities promptly notify affected individuals of a breach (unless an exception applies), to notify the Secretary of HHS and the media of certain large breaches, and to file with HHS an annual report of breaches. On January 25, 2013, HHS promulgated the Omnibus Rule which, among other things, modified the breach notification regulations, including the definition of the term "breach."

DEFINITIONS:

"Breach" means the acquisition, access, use or disclosure of protected health information (PHI), in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

Breach excludes:

- An unintentional acquisition, access or use of PHI by a member of the AHS workforce or business associate (BA), if such acquisition, access or use was made in good faith, was within the scope of authority, and does not result in further impermissible use or disclosure.
- An inadvertent disclosure by a member of the AHS workforce who is authorized to access PHI to another member of the AHS workforce (or, in the case of a Business Associate, to another member of the BA workforce) who is also authorized to access the PHI, and the information received is not further used or disclosed.
- A disclosure of PHI where AHS (or one of its BAs) has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

SCOPE:

This policy applies to all AHS employees, including exempt, classified, temporary and contractual, and certain volunteers.

STANDARDS and/or GUIDELINES:

Employees' responsibilities:

1. Employees will learn their responsibilities under HIPAA and AHS Rule #08-048. They should understand the circumstances in which they can properly share consumers' PHI with other AHS employees and/or persons who are outside of AHS. They must take precautions to avoid others improperly accessing PHI under their control. If an employee is unsure about whether s/he can share PHI with another person or entity, s/he must ask his/her supervisor, HIPAA liaison, the HIPAA privacy officer or AHS privacy officer (hereinafter collectively referred to as "privacy officer").
2. When employees improperly view PHI or share it with someone else, intentionally or unintentionally, they must **promptly** report the violation to the privacy officer and the HIPAA liaison for their department, unless the violation falls within one of the exceptions listed in the definitions above. HIPAA privacy and security event reporting forms can be found on the AHS intranet. (Alternatively, employees may report directly to their division's HIPAA liaison, who may fill out and send the event form.)
3. Employees will cooperate with their supervisor, their HIPAA liaison and Human Resource (HR) Administrator, the privacy officer and any other person investigating the circumstances of a HIPAA violation in which they were involved.
4. Employees will report, as in #2 above, when they are aware that another employee was responsible for a violation and did not report it.

Supervisors' responsibilities:

1. Supervisors will ensure that the employees they supervise have taken the AHS HIPAA training and remain aware of their responsibilities under HIPAA and AHS Rule #08-048.
2. Supervisors will assist their supervisees in determining if a situation constitutes a HIPAA violation that requires reporting. If they have questions about this, they will contact their HIPAA liaison or the privacy officer.
3. Supervisors will promptly report all improper HIPAA violations of which they are aware, unless the employee involved has already made such a report. They will remind their supervisees that violations must be brought to the privacy officer's attention as soon as possible.
4. When necessary, supervisors will assist their department's HIPAA liaison and HR Administrator, the privacy officer and any other person investigating the circumstances of a violation in which one of their supervisees was involved.
5. When the privacy officer determines that an employee's conduct violated HIPAA, regardless of whether the violation constituted a breach, when necessary the employee's supervisor may consult with the privacy officer and the HR Administrator concerning 1) a plan to mitigate any harm to the affected individual(s), if warranted, 2) a plan to ensure that the employee understands that his/her conduct violated HIPAA, and corrective action to be taken by the employee and/or the division, if appropriate, and 3) whether a sanction is warranted and, if so, the type of sanction.
6. After the consultation, above, and when appropriate, the supervisor will implement the mitigation plan agreed upon.
7. After the consultation, in #5 above, and when appropriate, the supervisor will ensure that the employee understands that his/her conduct violated HIPAA, and will implement any agreed upon corrective action plan to ensure that future violations do not occur.

HIPAA liaisons' responsibilities:

1. Liaisons will answer questions from employees and supervisors about actual or potential HIPAA violations and/or refer such questions to the privacy officer.
2. When they receive an event form concerning a HIPAA violation within their department, liaisons will promptly review the form and consult with the privacy officer about the facts of the event and the level of harm the improper use or disclosure poses to the affected individual(s). If the facts of the event are not clearly known or are in dispute, the liaison will assist the privacy officer and/or the HR administrator in an investigation, as appropriate.

HR Administrators' responsibilities:

1. If an investigation into the potential HIPAA violation is necessary, HR Personnel assigned to support the employee's department will assist the employee's supervisor in following the procedure in place for investigating alleged employee misconduct and ensure a factual account is provided to the privacy officer.
2. When the privacy officer has determined that an employee's conduct violated HIPAA, regardless of whether the conduct constituted a breach, and the conduct also constituted a personnel policy violation, the HR Administrator for the employee's department will consult with the privacy officer and the employee's supervisor concerning 1) a plan to mitigate any harm to the affected individual(s), 2) a plan to ensure that the employee understands that his/her conduct violated HIPAA and corrective action, if appropriate, and 3) whether a sanction is warranted (not all HIPAA violations will warrant a sanction) and, if so, the type of sanction should be recommended to the employee's Appointing Authority.
3. After the consultation, above, if the privacy officer and/or the employee's supervisor cannot agree with the proposed sanction, the Appointing Authority or their designee or the head of the department or division, as applicable, will determine the appropriate sanction.

Privacy Officers' responsibilities:

1. The privacy officers will answer all questions from employees, supervisors and liaisons about actual or potential HIPAA violations and breaches.
2. The privacy officers will review all HIPAA event forms and complaints about HIPAA violations from the public. The privacy officers will decide whether further investigation is required in order to determine whether the employee's conduct violated HIPAA and, if so, whether it constituted a breach as defined above.
3. In situations in which a possible violation is referred to HR for further investigation of the facts, a privacy officers may participate in the investigation.
4. When making the determination as to whether an employee's HIPAA violation constituted a breach, a privacy officer will conduct an analysis concerning whether there is a low probability that the PHI has been compromised, using the risk factors set forth in the Privacy Rule. The privacy officer will consult with the employee's supervisor and/or department liaison, as appropriate. The privacy officer will document the risk analysis.
5. When a privacy officer determines that a violation has occurred and there is not a low probability that the PHI has been compromised, the privacy officer will ensure that the impacted individual(s) is sent written notice of the breach as soon as possible and in no case later than 60 days after the breach was known to any AHS employee.

6. When a privacy officer determines that an employee's conduct violated HIPAA, regardless of whether the violation constituted a breach, the privacy officer will consult with the employee's supervisor and HR administrator concerning 1) a plan to mitigate any harm to the affected individual(s), 2) a plan to ensure that the employee understands that his/her conduct violated HIPAA and corrective action, if appropriate, and 3) whether a sanction is warranted and, if so, the type of sanction.

7. After the consultation, above, the privacy officer will ensure that any mitigation plan is implemented.

8. A privacy officer will keep a log of all HIPAA event reports and complaints from the public. At the beginning of each calendar year, in accordance with HHS regulations, the privacy officer will send a report to HHS of all breaches that did not fall within one of the exceptions that occurred in the last calendar year.

COMPLIANCE:

Employee (including volunteer) adherence to this policy is the shared responsibility of supervisors and managers, HIPAA liaisons for each department and division, and the HIPAA Privacy Officer for AHS.

ENFORCEMENT:

The Office of the Secretary of the Agency may initiate reviews or assessments or take other steps to ensure that this policy is being followed.