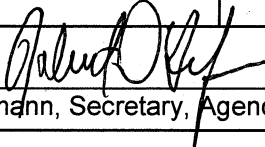


STATE OF VERMONT
Agency of Human Services (AHS)

HIPAA Breach Notification	REVISION HISTORY:	Chapter/Number 6.03
	EFFECTIVE DATE: 6/4/10	Attachments/Related Documents:
Authorizing Signature: <u></u> Date Signed: <u>6/4/10</u> Robert D. Hofmann, Secretary, Agency of Human Services		

PURPOSE/POLICY STATEMENT: To notify and protect individuals whose personally identifiable health information is breached, as that term is defined below. When the Agency of Human Services (AHS) determines that there is a significant risk of harm from a breach, AHS will promptly notify the affected individuals so that they are aware of the breach and have the opportunity to take steps to protect themselves from the consequences of it. When AHS determines that there is not a significant risk of harm to the affected individuals, AHS will not notify the individuals.

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). These regulations, found in 45 CFR, part 164, subpart D, implement provisions of the American Recovery and Reinvestment Act passed on February 17, 2009. The new regulations define the term breach. They require Covered Entities to promptly notify affected individuals of the 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. In the past, AHS had no legal obligation to notify consumers of HIPAA breaches, but did so in cases in which it determined that there was potential harm that could result from the 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 poses a significant risk of financial, reputational or other harm to the individual.

Breach excludes:

- An unintentional acquisition, access or use of PHI by an AHS employee 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 person who is authorized to access PHI to another person at AHS (or, in the case of a BA, to another person at the same BA) 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.

STANDARDS and/or GUIDELINES:

Employees' responsibilities:

1. Employees will learn their responsibilities under HIPAA and AHS Rule #08-048. They must understand the circumstances in which they can properly share consumers' PHI with other 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 or the AHS 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 AHS 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 supervisors, who shall fill out and send the event form.)
3. Employees will cooperate with their supervisor, their department's 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.

Supervisor's 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 AHS 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 who is 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, the employee's supervisor will 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, the supervisor will implement the mitigation plan agreed upon.
7. After the consultation, in #5 above, 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 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 the employee involved in a potential HIPAA violation does not admit to the facts as alleged in the internal report or complaint from a member of the public, or if the facts are not clear, the HR administrator for the employee's department will investigate the matter and will provide a factual account 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, 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 and, if so, the type of sanction.
3. After the consultation, above, the HR administrator will propose a sanction (not all HIPAA violations will warrant a sanction). If the privacy officer and/or the employee's supervisor do not agree with the proposed sanction, the head of the department or division will decide on the appropriate sanction.

Privacy Officer's responsibilities:

1. The privacy officer will answer all questions from employees, supervisors and liaisons about actual or potential HIPAA violations and breaches.
2. The privacy officer will review all HIPAA event forms and complaints about HIPAA violations from the public. The privacy officer 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. If further investigation of the facts is required, the privacy officer will refer the matter to the appropriate HR administrator. The privacy officer may participate in the investigation.
4. Based upon the facts as admitted, or as found by the HR administrator after an investigation, the privacy officer will determine whether the employee's conduct 1) violated HIPAA and 2) if so, whether the conduct constituted a breach, and 3) if so, whether any of the exceptions to the breach notification requirements apply. The privacy officer will so inform the employee's supervisor, the department's HR administrator and the HIPAA liaison.
5. When making the determination as to whether an employee's HIPAA violation constituted a breach, the privacy officer will conduct an analysis of the level of risk of financial, reputational or other harm to the affected individual(s). The privacy officer will consult with the employee's supervisor and/or department liaison, as appropriate. The privacy officer will document the risk analysis.

6. When the privacy officer determines that a violation poses a significant risk of harm to the affected individual(s) and none of the exceptions to the breach notification requirement apply, the privacy officer will ensure that the 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.
7. When the 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.
8. After the consultation, above, the privacy officer will ensure that any mitigation plan is implemented.
9. The 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.