



# HURON BEHAVIORAL HEALTH OPERATIONAL POLICY

Policy #: **ORI.1.31**  
Issue Date: 12/02/09  
Rev. Date: 03/28/17  
Page: 1 of 6

## Title: Breach Notification Policy

Prepared By: Compliance Officer

NOTE: This Document Copy is **Uncontrolled and Valid on this date only: April 4, 2017**. For Controlled copy, view shared directory I:\ drive

### Purpose:

To define the process and protocols for employees to take when a known or suspected breach of confidentiality has occurred, in accordance with 45 CFR (sections 164.404, 164.406, & 164.408).

### Scope:

This policy applies to all employees (including full-time employees, part-time employees, contractual providers, volunteers, students or interns), of Huron Behavioral Health (HBH) and all consumers served.

### Information:

1. On January 17<sup>th</sup>, 2013, the United States Department of Health and Human Services (HHS) released the HITECH (Health Information Technology for Economic and Clinical Health) Final Rule which further restricts health care providers, health plans, and other entities covered under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (45 CFR) to notify individuals when their health information is breached. These "breach notification" regulations implement provisions of the HITECH Act, passed as part of the American Recovery & Reinvestment Act of 2009 (ARRA).
2. The breach notification provisions of the HITECH Act apply to HIPAA-covered entities and their business associates who access, maintain, retain, modify, store, destroy, or otherwise hold, use, or disclose PHI.
3. These regulations, developed with the HHS Office for Civil Rights (OCR), require health care providers and other HIPAA-covered entities to promptly notify affected individuals of a breach of confidentiality, as well as the HHS Secretary and the media in cases where a breach affects more than five hundred (500) individuals. Breaches affecting fewer than five-hundred (500) individuals are to be reported to the HHS Secretary on an annual basis. Since business associates are also covered under the provision of the HITECH Act, all business associates of HBH are also required to notify HBH of any known or suspected breaches of confidentiality.
4. Huron Behavioral Health (HBH) is a covered entity and is required to comply with, including but not limited to, 45 CFR Sections 164.404, 164.406 and 164.408 concerning breaches of Protected Health Information (PHI).
5. Specifically, and according to these provisions, following a discovery of a breach of unsecured PHI, HBH is required to notify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach. (See "Definitions" section below for definition of "unsecured PHI".) Other notifications must also be made as detailed below.
6. All HBH employees receive annual Recipient Rights and Corporate Compliance training which includes training on confidentiality, disclosure, employee code of conduct, and employee disciplinary actions/sanctions for non-compliance (see also "HBH Training Requirements Procedure" TR.2.03).

### Policy:

#### A. Safe Harbor from Breach Notification Reporting:

1. Regardless of whether or not something is considered a breach, the HIPAA/HITECH Final Rule establishes a safe harbor for any breach of PHI that is encrypted according to federal guidelines. As long as the PHI involved in the breach was encrypted, there is no requirement to provide notification.

#### B. Individual Notification:

1. Following the discovery of a breach of unsecured PHI, HBH is required to notify the affected consumers (or their next of kin if the consumer is deceased) whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed in the breach. This notification must occur without unreasonable delay but no later than sixty (60) calendar days of the discovery of the breach. (Except when the

**Title: Breach Notification Policy**

Prepared By: Compliance Officer

Policy #: ORI.1.31

Issue Date: 12/02/09

Rev. Date: 03/28/17

Page: 2 of 6

NOTE: This Document Copy is **Uncontrolled and Valid on this date only: April 4, 2017**. For Controlled copy, view shared directory I:\drive

delay is required by a law enforcement official who determines that a notification would impede a criminal investigation or cause damage to national security.) The notification shall be written in plain language and include, to the extent possible:

- A brief description of what happened, date of the breach, and date of discovery of the breach, if known;
  - A description of the types of PHI involved (e.g. full name, social security number, address, diagnosis, and other types of information involved);
  - Any steps that individuals should take to protect themselves from potential harm as a result of the breach;
  - A brief description of what HBH is doing to investigate the breach, mitigate harm and to protect against future breaches;
  - Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, website and/or postal address.
2. This notification must be provided in plain language. In general, the written notification should be provided by first-class mail to the last known address of the person (alternatively, written notice may be provided in the form of an e-mail if the individual has agreed to electronic notice and the agreement has not been withdrawn). In situations where HBH believes the possibility exists for imminent misuse of the unsecured PHI, HBH may provide notice of the breach to affected consumers by telephone in addition to the written notice. If the individual is a minor or legally incapacitated, notice to the parent or personal representative is acceptable.
  3. If there is insufficient contact information for some or all of the affected individuals or if some of the notices are returned as undeliverable, substitute notice should be provided to the unreachable individuals in a manner reasonably calculated to reach them. For example, if HBH does not have the individual's last known address, but has the individual's email or telephone number, notice can be provided electronically or by phone without the individual's consent. Posting a notice on HBH's website may also be appropriate.
  4. In the case where there is insufficient or out-of-date contact information, HBH will provide substitute notice, including, when there are ten (10) or more individuals for whom there is insufficient contact information, a conspicuous posting on the HBH website for at least ninety (90) days, or a notice in a major print (such as a state or local newspaper or magazine) or using a broadcast media in the geographic area(s) where the affected individuals likely reside. The notice must include a toll-free telephone number that remains active for at least ninety (90) days for individuals to call regarding the breach.

**C. Media Notification:**

1. In addition to notifying affected individuals of the breach, when a breach of unsecured PHI involves more than five-hundred (500) consumers, HBH shall provide notice to appropriate prominent media outlets serving the state or jurisdiction. This will be done without unreasonable delay following discovery of the breach (in no case later than sixty days after discovery). This would typically be in the form of a press release to appropriate media outlets such as a general interest newspaper with daily circulation covering the area where the affected individuals live. The information required for the notification will contain the same information as discussed above for individual notification (see item B.1 above).

**D. Government Notification:**

1. **500 or more individuals:** For breaches of unsecured PHI involving five-hundred (500) or more individuals, HBH shall also provide notice to the government within sixty (60) days of the breach, contemporaneously with the notifications to the individuals, in the manner specified on the HHS website. HBH will utilize the HHS electronic report form and the reporting instructions/format specified by HHS @ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.
2. **Less than 500 individuals:** For breaches involving less than five-hundred (500) individuals, HBH shall maintain a record-log using the "[Breach Notification Log Form](#)" (90-468) and shall report this information to HHS on an annual basis (no later than 60 days after the end of each calendar year). HBH will utilize the electronic report form and the reporting instructions/format specified by HHS @ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

**Title: Breach Notification Policy**

Prepared By: Compliance Officer

Policy #: **ORI.1.31**

Issue Date: 12/02/09

Rev. Date: 03/28/17

Page: 3 of 6

NOTE: This Document Copy is **Uncontrolled and Valid on this date only: April 4, 2017**. For Controlled copy, view shared directory I:\drive

**E. Process for Employees when a Suspected or Known Breach of Confidentiality has Occurred:**

1. If any HBH employee becomes aware of any issue or matter that could possibly impact HBH's breach notification obligations, the employee must immediately report the information to the HBH Compliance Officer using any of the following methods:
  - Phone reporting: Levi Zagorski direct line at (989) 269 - 1122
  - E-mail reporting: levi@huroncmh.org
  - In writing to: Huron Behavioral Health  
P.O. Box 312  
Bad Axe, Michigan 48413  
Attention: Compliance Officer
2. Employees are not expected nor should they attempt to make a determination as to whether an actual breach (as defined in the "Definitions" section below) has taken place. Rather, employees are expected to report any known or suspected instances where PHI may have been accessed or disclosed inconsistent with the HIPAA privacy regulations and HBH's "Minimum Necessary Protocols for External Disclosures Policy" (ORI.1.13) and "Minimum Necessary Protocols for Internal Disclosures Policy (ORI.1.14) Failure to report a known or suspected breach is a violation of this policy and can result in disciplinary action in accordance with HBH's discipline/employment policies and procedures. (see also ORI.1.08 "Compliance Internal Reporting Policy" and "Employee Code of Conduct Policy" ORI.1.18).
3. Examples of issues that should be reported for further investigation include, but are not limited to:
  - Access of data/files/records by unauthorized individuals;
  - Access of data/files/records by authorized individuals but for improper non-business purposes;
  - Disclosure of data/files/records to unauthorized individuals;
  - Disclosure of PHI without an authorization when an authorization is required; and
  - Disposing of PHI such as hardcopy reports or other paper containing PHI without following appropriate destruction protocols (e.g. failure to shred reports prior to disposal) (see also QI.1.23 "HBH Record Retention and Storage Policy")
4. Upon receipt of a report, the Compliance Officer will notify the Executive Director and will conduct an investigation to determine whether HBH has a notification obligation under the regulations.
5. It is also HBH's policy and a requirement of our business associate agreements that all business associates, subcontractors, or vendors must report (within forty-eight hours) any breach of confidentiality consistent with this policy.

**F. Procedure for Investigating a Breach:**

Upon receipt of a report or learning of an issue that may impact HBH's breach notification obligations, the Compliance Officer (and additional staff, as appropriate) shall do the following:

1. **Investigate the Breach:** Conduct an investigation to determine if the matter involved unsecured PHI (as defined in the "Definitions" section below). If the matter involved unsecured PHI, the Compliance Officer, and other staff as appropriate, shall determine whether or not a breach has occurred. The following actions shall be taken by the Compliance Officer and/or other HBH staff:
  - a. Determine whether there has been an impermissible use or disclosure under the privacy regulations. The Compliance Officer shall gather and document all relevant facts and circumstances pertinent to the issue and conduct a risk assessment, which includes:
    - the nature and extent of PHI;
    - whether the PHI is individually identifiable;
    - the types of identifiers and the likelihood of re-identification;

**Title: Breach Notification Policy**

Prepared By: Compliance Officer

Policy #: ORI.1.31

Issue Date: 12/02/09

Rev. Date: 03/28/17

Page: 4 of 6

NOTE: This Document Copy is **Uncontrolled and Valid on this date only: April 4, 2017**. For Controlled copy, view shared directory I:\drive

- the unauthorized person who accessed/obtained PHI or to whom the disclosure was made (for example if the person to whom the PHI was improperly disclosed is another HIPAA-covered entity who is also obligated to protect PHI. In this case there would be a determination that there is a low probability that the PHI was compromised);
  - whether the PHI was actually acquired or only viewed (for example, a laptop containing unencrypted PHI is lost, but later found and forensic analysis reveals that the PHI was never accessed, this would favor a determination that no notification is required), and;
  - the extent to which any risk of PHI has been mitigated (if PHI is improperly used or disclosed, HBH or the business associate should immediately take steps to mitigate any potential risk to the PHI, which would favor a determination that there is a low probability that the PHI was compromised)
- b. If there has been an impermissible use or disclosure, HBH must determine and document whether the impermissible use or disclosure compromises the security or privacy of the PHI and is considered to be a reportable breach after conducting the risk analysis (i.e. HBH has determined that there is a high probability that the PHI has been compromised based on a risk assessment) that it poses a significant risk of financial, reputational, or other harm to the individual). Legal counsel should be consulted at this stage. If the risk assessment indicates a low probability of compromise, no notification is required.
- c. A determination must be made as to whether or not the breach is considered excluded. A breach is excluded if:
- There is an unintentional acquisition, access, or use of PHI by a workforce member or a person acting on behalf of HBH. If such acquisition, access or use was made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the privacy regulations; or
  - Any inadvertent disclosures by a person who is authorized to access PHI to another person authorized to access PHI and the information is not further used or disclosed in a manner not permitted under the privacy regulations; or
  - A disclosure of PHI where HBH 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.

Note that under the regulations, HBH retains the burden of proof to show why the matter falls under one of the above three (3) exceptions. Legal counsel should be consulted when making this determination.

Note: The Compliance Officer may consult with legal counsel as part of the process to assist in analyzing the issues and in making determinations as to appropriate reporting

- 2. Report the Breach:** If the results of the investigation reveal that a reportable breach has occurred, the Compliance Officer and/or other appropriate administrative staff is required to make notification without unreasonable delay but no later than sixty (60) calendar days of the discovery of the breach in accordance with items B, C, and D above. Additionally, if a reportable breach has occurred, HBH will immediately report the breach to the Mid-State Health Network (MSHN) in accordance with contractual obligations.

**Definitions/Acronyms:**Acronyms:

ARRA – American Recovery and Reinvestment Act

CFR – Code of Federal Regulations

ePHI – Electronic Protected Health Information

HBH – Huron Behavioral Health

HHS – Health and Human Services

HIPAA – Health Insurance Portability &amp; Accountability Act

HITECH – Health Information Technology for Economic and Clinical Health

PHI – Protected Health Information

## Title: Breach Notification Policy

Prepared By: Compliance Officer

Policy #: ORI.1.31

Issue Date: 12/02/09

Rev. Date: 03/28/17

Page: 5 of 6

NOTE: This Document Copy is **Uncontrolled and Valid on this date only: April 4, 2017**. For Controlled copy, view shared directory I:\drive

### Definitions:

**Breach:** means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the privacy or security of the information. In order for a breach to occur, the acquisition, access, use, or disclosure must be in violation of the HIPAA Privacy Rules and which compromises the security or privacy of consumer's PHI (i.e. a risk assessment has been done to determine if there is a low or high probability of a compromise of the PHI). Note that a breach would not be considered to pose a significant risk if the PHI at issue does not include certain identifiers. Identifiers in the Privacy Rule (45 CFR) include the following:

- Date of Birth
- Names
- Social Security Numbers
- Case Numbers
- Account Numbers
- Health Plan Numbers
- Addresses (other than town/city or state)
- Certificate/Licensure Numbers
- Vehicle Identifiers
- Telephone Numbers
- Telefax Numbers
- E-mail Addresses
- Full-face Images & comparable images
- Biometric Identifiers
- Internet Protocol Address Numbers
- URLs
- Device Identifiers & Serial Numbers
- Genetic Information

**Encryption:** Algorithms that encode plain text into non-readable form providing privacy. The receiver of the encrypted text must use a "key" to decrypt the message which then returns it to its original plain text form. Encryption technology is intended to make PHI private.

**Exceptions/Excluded Breach:** For the purpose of this policy, it is not considered a breach if:

- (a) there is an unintentional acquisition, access or use of PHI by a workforce member or a person acting on behalf of HBH 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 a further use or disclosure in a manner not permitted under the privacy regulations (example: an employee mistakenly sends an e-mail with PHI to another co-worker who opens it in the normal course of business but then deletes it and notifies the first employee); or
- (b) an inadvertent disclosures by a person who is authorized to access PHI at HBH or a business associate to another person authorized to access PHI at HBH and the information is not further used or disclosed in a manner not permitted under the privacy regulation; or
- (c) a disclosure of PHI where HBH 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. (An example would be if HBH sent a record to an incorrect consumer. The document is returned to HBH by the post-office as undeliverable and is unopened. In such a case, HBH can conclude that the incorrect addressee could not have retained the PHI.)

Note that under the regulations, HBH retains the burden of proof to show why the matter falls under one of the above three (3) exceptions.

**Genetic Information:** relates to genetic tests of the person or peros family members, the manifestation of a disease or disorder in the person's family members, or any requests for receipt of genetic services, or participation in clinical research which includes genetic services, by the person or any family member of the person.

**Protected Health Information:** is individually identifiable health information including demographic data, that relates to the individual's past, present, or future physical or mental health condition, the provision of healthcare to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g. name, address, date of birth, social security number, etc.)

**Unsecured PHI:** is defined as all PHI except ePHI secured through encryption, and ePHI or paper PHI that has been destroyed (that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology set forth in HHS guidance.

### **Forms:**

[90-468 Breach Notification Log Form](#)

### **Records:**

Records of Breaches of Confidentiality are retained by the Compliance Officer for a minimum of seven (7) years. Records of risk analyses are maintained in the Compliance Concern database for a minimum of ten (10) years. Training records are retained by the HBH Training Manager (or designee) for seven (7) years.

**Title: Breach Notification Policy**

Prepared By: Compliance Officer

**Policy #: ORI.1.31**  
**Issue Date: 12/02/09**  
**Rev. Date: 03/28/17**  
**Page: 6 of 6**

NOTE: This Document Copy is **Uncontrolled and Valid on this date only: April 4, 2017**. For Controlled copy, view shared directory I:\drive

**Reference(s) and/or Legal Authority**

45 CFR (Sections 164.404, 164.406, 164.408) @ <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>  
 NIST Computer Security Standards (Federally Approved Guidelines for Media Sanitation) @ [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)  
[ORI.1.08 Compliance Internal Reporting Policy](#)  
[ORI.1.13 Minimum Necessary Protocols for External Disclosures Policy](#)  
[ORI.1.14 Minimum Necessary Protocols for Internal Disclosures Policy](#)  
[ORI.1.18 Employee Code of Conduct Policy](#)  
[QI.1.23 HBH Record Retention and Storage Policy](#)  
[TR.2.03 HBH Training Requirements Procedure](#)

**Change History:**

Change Letter	Date of Change(s)	Changes
None		New policy to comply with 45 CFR (164.404, 164.406, and 164.408) and the new HITECH regulations effective August 24, 2009.
A	05/07/13	Reviewed and revised to comply with 8 <sup>th</sup> edition COA standards – in D.1 changed contact information from Sue Healy to Catherine Jaskowski, added "HITECH" to "Acronym" section; no other content changes.
B	08/15/13	Reviewed and revise to comply with recent HIPAA/HITECH legislative changes – added "Genetic Information"(to Breach Definition), added "Protected Health Information", and "Encryption" "Breach" to "Definitions", added bullets in E.1.a, added second sentence in "Records" section, added A to "Policy" section, in B.2 added "(alternatively...)" and last sentence, added B.3, in B.4 added "for at least 90 days" and last sentence, in C.1 added "such as a general interest newspaper....", added F.1.a. in F.1.b added "(i.e. HBH has determined....)", added "ePHI" to "Acronym" section.
C	04/21/15	In E.1 removed "Catherine Jaskowski" and replaced with "Levi Zagorski" & corrected email address, no other content changes made.
D	05/27/15	Revised to comply with MSHN 2015 Delegated Managed Care Audit – added last sentence in F.2 to clarify existing practices.
E	03/28/17	In C.1 removed "The notice can be in the form of a press release." As it was a repeat statement in this section, in E.4 added "and notify the Executive Director, changed "Compliance Liaison" to "Compliance Officer" (13 places), in "References" section and E.2 added "ORI.1.18, made several additional minor wording/grammatical changes/corrections throughout document without changing sentence content.