STATE OF CONNECTICUT
Department of Mental Health & Addiction Services

Department of Mental Health and Addiction Services

Commissioner's Policy Statement and Implementing Procedures

SUBJECT:	Unauthorized Disclosure & Breach Notification of Unsecured PHI
P & P NUMBER:	Chapter 3.13
APPROVED:	Patricia Rehmer, Commissioner Date: September 23, 2013
EFFECTIVE DATE:	September 23, 2013
REVISED:	September 23, 2013
REFERENCES:	ARRA Title XIII Section 13402 45 CFR, Parts 160 and 164 CT Gen. Stat. §36a-701(b)
FORMS AND ATTACHMENTS:	Breach Notification Risk Assessment Tool (Exhibit A) HHS Breach Notification Form (Exhibit B)

STATEMENT OF PURPOSE: This policy establishes the actions that the Department of Mental Health and Addiction Services (DMHAS) as a covered entity defined under The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations at 45 C.F.R. Parts 160 and 164, as amended (HIPAA) and Subtitle D of the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§17931-39 (HITECH) must take in identifying, managing and responding to potential and confirmed breaches of unsecured protected health information (PHI).

POLICY: The DMHAS is committed to mitigating the risks associated with the impermissible use, inadvertent loss or unauthorized disclosure of PHI. It is the policy of the DMHAS to respond to, and provide notifications, when required by law, of breaches of PHI and to document its approach and response to such breaches. The DMHAS will manage potential and actual breaches of unsecured PHI in accordance with the procedures that follow.

PROCEDURE: The DMHAS must take the following actions as soon as an impermissible use, unauthorized disclosure of PHI and/or potential breach has been discovered to determine if a privacy or security incident constitutes a reportable breach under HIPAA and HITECH.

A. Analysis-General

1. Determine and document whether there has been impermissible use or unauthorized disclosure of PHI under the Privacy Rule.

2. Determine and document whether the incident falls under one of the breach exceptions as defined in Appendix A

3. If there has been impermissible use or disclosure of PHI under the Privacy Rule that does not qualify for one of the exceptions, determine and document whether such impermissible use or disclosure compromises the security or privacy of PHI by conducting a risk assessment as described in Section D below.

B. Reporting Actual/Suspected Unauthorized Use or Disclosure of PHI

1. Workforce Member - In the event of an actual or suspected unauthorized use or disclosure discovered by a workforce member or communicated to the workforce member, that person shall immediately notify the Facility Compliance and/or Privacy Officer, who shall report the incident to the Facility Chief Executive Officer (CEO)

2. Business Associate - In the event DMHAS receives notification of suspected or actual unauthorized use or disclosure of PHI from a Business Associate, whereas the DMHAS is the Covered entity, notification must be directed to the Agency Compliance and Privacy Officer. The Agency Compliance and Privacy Officer will investigate the unauthorized disclosure and convene the IRT.

3. Following the discovery of an actual or suspected breach, the DMHAS shall begin an investigation, conduct a risk assessment and begin making necessary notifications, if necessary.

C. Incident Investigation

1. The DMHAS shall begin an investigation upon discovery of potential impermissible use or unauthorized disclosure of PHI.

2. The Facility Compliance Officer, the Facility Privacy Officer (for non-electronic violations) and the Facility Security Officer (for Information Security violations) shall convene an Incident Response Team (IRT) who shall be responsible for investigating and responding to all actual or suspected breaches.. The respective teams will collaborate with responsible senior management and others as appropriate.

D. Risk Assessment

1. The Facility Compliance Officer shall direct and perform a risk assessment to determine if a breach occurred and if notifications to individuals and/or the media re required.

2. The DMHAS facility shall notify the Agency Compliance and Privacy Officer (ACPO) that a possible breach has been discovered and a risk analysis has commenced. The facility may request assistance and/or legal support. Each facility must use the Breach Notification Risk Assessment Tool in Exhibit A.

3. As part of the incident investigation the facility must conduct a risk assessment to determine if there is a violation of the Privacy Rule that "compromises the security or privacy of the PHI". Impermissible use or disclosure of PHI that does not qualify for an exception is presumed to be a breach pending further analysis.

4. Risk assessment must consider, at a minimum, the following four factors:
    - The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification
    - The identity of the unauthorized person who used the PHI or to whom the disclosure of PHI was made
    - Whether the PHI was actually viewed or acquired or, alternatively, if only the opportunity existed for the information to be viewed or acquired
    - The extent to which the risk to the PHI has been mitigated

5. The risk assessment shall consider if an exception to the definition of Breach applies. Specifically, a "breach" does not include:

    - Any "unintentional" acquisition, access or use of PHI by a workforce member or individual acting under the authority of the covered entity or business associate that is made in good faith, within the course or scope of employment or other professional relationship, and is not further used or disclosed in an unlawful manner under the HIPAA Privacy Rule
    - An "inadvertent" disclosure by a person who is authorized to access PHI to another authorized person at the same covered entity, business associate or organized healthcare arrangement, and the PHI is not further used or disclosed in an unlawful manner under the HIPAA Privacy Rule
    - A disclosure of PHI where the covered entity or business associate had a good-faith belief that the unauthorized person to whom the information was disclosed would not reasonably be able to "retain" such information
    - The unauthorized acquisition, access, use or disclosure of PHI that has been completely de-identified in accordance with HIPAA
    - The unauthorized acquisition, access, use or disclosure of electronic PHI that has been secured.

6. Based on the outcome of this investigation, including risk assessment, the IRT will determine whether there has been a breach under HIPAA/HITECH and in the case of a confirmed breach will coordinate providing requisite notice(s) to individuals, HHS Secretary and media in accordance with the procedure in Section E below.

7. The ACPO will confirm with in house legal counsel and/or the Attorney General's Office any determinations that were deemed a non-breach or unauthorized disclosure based on the DMHAS analysis.

8. Documentation of the investigation, including the risk assessment will be maintained in the facility. Upon completion, a copy of the risk assessment must immediately be forwarded to the ACPO.

E. Maintenance of Breach Documentation

The Facility Compliance Officer shall document each actual or suspected breach including, but not limited to, the details of the Breach, the response, the risk assessment, the outcome, steps taken to mitigate harm and any changes to DMHAS's Risk Analysis or security procedure to avoid reoccurrence of the breach. All such documentation shall be retained in accordance with the State of Connecticut Record Retention Schedule/

Following determination of a breach by the IRT the facility Compliance and/or Privacy Officer will complete the HHS Breach Notification Form in conjunction with individuals involved. (Exhibit B) A copy of the form and a record of submission will be sent to the ACPO.

If it is determined that no breach occurred, the documentation and all associated paperwork shall be retained by the DMHAS facility and a copy sent to the ACPO. All documentation shall be kept according to the State of Connecticut Record Retention Schedule.

F. Notice to Individuals & Methods of Notification

In the event of a confirmed breach of unsecured PHI for less than 500 individuals, the following persons will be notified in the manner described below. This Policy does not prevent a covered entity from notifying individuals when PHI is inappropriately disclosed, but an investigation determines that the incident does not give rise to a mandatory report under HITECH:

Notice to Affected Individual(s). Notice to the affected individual(s) shall be made without unreasonable delay and in no case later than (60) sixty calendar days of the discovery of the breach. At the direction of the Facility Compliance Officer upon consultation, as needed, with the ACPO in conjunction with the DMHAS legal department and/or the Attorney General, notice shall be provided to individuals whose PHI was reasonably believed to have been involved in the breach.

Notice shall be provided in the following form:

(a) *Sufficient/up-to-date Contact Information*. Written notification by first-class mail to the individual, or in the case of a minor, or other individual who lacks legal capacity, to the parent or other person who is the personal representative of 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 should be provided in one or more mailings as information is available. If the covered entity knows that the individual is deceased and has the address of the next of kin or personal representative, the covered entity shall provide notice by first-class mail to the next of kin or personal representative.

(b) *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, the covered entity shall provide a substitute form of notice reasonably calculated to reach the individual. A substitute notice does not need to be provided if there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

(i) If 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, including posting notice on covered entity's Web site.

(ii) If 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 the covered entity's Internet site(s) or a conspicuous notice in major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach. The DMHAS Public Information Officer, after consultation with the agency Compliance and Privacy Officer is responsible for notifying media outlets and the Web Master for posting on the web site.

(c) If the organization 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 written notice described above.

(d) Except when law enforcement requests a delay as provided in Section H below, following discovery of a breach, the covered entity shall notify each affected individual without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. It is the responsibility of the covered entity to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

1. Notice to Media. For breaches involving 500 or more residents of a particular State or jurisdiction (County, City or Town), the DMHAS Public Information Officer after consulting with the Agency Compliance and Privacy Officer, as well at the Attorney General's Office, will provide notice to prominent media outlets serving such state or jurisdiction without unreasonable delay and in no case later than (60) sixty calendar days after discovery of the breach. The notice may be provided in the form of a press release and shall contain all of the information required by Section G of this Policy. This media notice supplements, but does not replace, individual written notice described above.

2. Notice to Secretary of HHS. In the event the risk assessment determines that a breach occurred, the Facility Compliance Officer shall notify the Secretary of HHS by submitting the approved HHS Breach Notification Form online at www.hhs.gov as follows:

   (a) For breaches involving 500 or more individuals, at the same time written notice is made to the affected individuals.

   (b) For breaches involving fewer than 500 individuals, no later than 60 days after the end of each calendar year.

3. Notice to State Attorney General Effective October 1, 2012 the State Attorney General will be notified of any breaches of unsecured PHI no later than the time when notice is provided to the resident of the State of CT.

G. Content of the Notification to Individuals

Any required notice shall be written in plain language and, to the extent possible, should contain the following information:

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 full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other identifying PHI or financial information)

3. Any steps the individual should take to protect themselves from potential harm resulting from the breach ;

4. A brief description of what the covered entity is doing to mitigate and investigate the breach, and to protect against further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, website, or postal address.

H. Permitted Delay in Notification

1. If a law enforcement official states to the covered entity that a required notification, notice, or posting would impede a criminal investigation or cause damage to national security, the covered entity shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time 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 notification, notice or posting for no longer than 30 days from the date of the oral statement, unless a written statement as described above is provided during that time.

I. Discovery of a Breach

A breach of unsecured PHI shall be treated as "discovered" as of the first day such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity (includes breaches by the organization's business associates). The 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 or entity committing the breach, who is a workforce member or agent (may include certain business associates) of the covered entity.

J.. Third Party Hosted PHI

Business associates also have an obligation to report breaches to the affected covered entity so that the covered entity can follow proper notification procedures. If, however, workforce members responsible for contracts which entail the maintenance of PHI on hosts belonging to a third party receive notice from third vendor (business associate) of any suspected or confirmed breach, s/he must immediately notify the Compliance and Privacy Officer.

K. Workforce Training

The DMHAS shall train workforce members on the procedures to take if they suspect or know of a breach.

FORMS AND DOCUMENTS
Breach Notification Risk Assessment Tool (Exhibit A)
HHS Breach Notification Form (Exhibit B)

REFERENCES
ARRA Title XIII Section 13402
45 CFR, Parts 160 and 164
CT Public Act 05-148
CT Gen. Stat. §36a-701(b)

APPENDIX A

DEFINITIONS

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

   (b) Breach excludes:

   (i) any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA), 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 under the HIPAA Privacy Rule.

   (ii) any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

   (iii) a disclosure of PHI where a CE or BA has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information (e.g., EOB sent to the wrong individual, but returned by Post Office unopened as undeliverable).

   (iv) The unauthorized acquisition, access, use or disclosure of PHI that has been completely de-identified in accordance with HIPAA

   (v) The unauthorized acquisition, access, use or disclosure of electronic PHI that has been secured.

2. The **"Electronic Data Incident Response Team (EDIRT)"** is a multidisciplinary task force composed of the Facility assigned Information Security Officer, the Director of IT, the Legal Department, and others as appropriate (e.g., Information Security, Human Resources – Employee Relations, Patients Relations, Public Relations, Protective Services/Security) responsible for investigating and responding to breaches including but not limited to external networks (for example, firewalls, web servers and VPNs); lost or stolen data storage media (for example laptops or desktop computer hard drives, USB attached devices such as thumb drives, smart phones); accidental release of electronic protected health information (EPHI) resulting from system malfunctions; the introduction of viruses into networks, etc.

3. **"Disclosure"** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

4. The **"Information Security Officer"** Each Facility will have an information security officer assigned to carry out the Information Security strategy, policies, and operations. This individual will be identified by the Director of IT.

5. **"Incident"** means any potential violation of the Privacy or Security Rule that warrants an investigation to determine if a breach has occurred.

6. **"Unauthorized Disclosure Incident Response Team (UDIRT)"** is a multidisciplinary task force composed of the Legal Department, ACPO and others as appropriate (e.g., Information Security, Human Resources – Employee Relations, Patient Relations, Public Relations, Protective Services/Security) responsible for investigating and responding to breaches of privacy policies; accidental release of protected health information.

7. **"Individually Identifiable Health Information"** means that information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

8. **"Law Enforcement Official"** means any officer or employee of a State agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. (45 CFR § 164.103)

9. **"Protected Health Information (PHI)"** means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

10. **"Unsecured Protected Health Information"** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the HHS Secretary guidance posted on the HHS website (i.e., encryption or destruction).

11. **"Use"** includes data in the process of being created, retrieved, updated, or deleted.

12. **"Workforce Member"** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, regardless of whether they are paid by the Agency.

13. **"Business Associate"** means a person or entity who, on behalf of DMHAS, and other than in the capacity of a workforce member: (i) creates, receives, maintains or transmits protected health information for certain functions or activities including claims

processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management and reprising; (ii) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services; (iii) provides data transmission services with respect to protected health information during which the person or entity requires more than routine access to such protected health information; or (iv) offers a personal health record to one or more individuals on behalf of DMHAS. Business Associate also means a subcontractor that creates, receives, maintains or transmits protected health information on behalf of the Business Associate.

14. **"Secured"** refers to PHI that is rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.

15. **"Risk Assessment"** means a systematic process of evaluating an incident to determine the likelihood that the incident will result in or cause certain outcomes, including whether an incident is a breach.

16. **"Discovery"** means the first day on which a breach is known to the covered entity or, by exercising reasonable diligence, would have been known to the covered entity. The covered entity 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 or entity, other than the person or entity committing the breach, who is a workforce member or agent of the covered entity.

Exhibit A

Breach Notification Risk Assessment Tool

Patient Name: **Patient's Legal Representative (if applicable):** **Medical Record Number:**	**Date of incident:** **Date of Discovery:**
Number of patients involved:	
Patient Relations contact: **Other DMHAS contact(s)**	**Phone #:** **Phone #:**
Brief Summary/Findings:	**Final Decision:** **Determined by:** **Date:**
Source of Incident: Who was responsible for the inappropriate access, use or disclosure ("incident")? *Circle your answer* If Business Associate is the source of the incident, enter the date the Business Associate notified DMHAS of the incident.	a) Internal to our organization b) Business Associate Date:
Are we the Business Associate? *Circle your answer* • If we are the Business Associate, enter the date we notified the other Covered Entity of the incident. • Enter the date that our organization became aware of the incident	a) Yes b) No Date Aware: Dated Notified:

NOTE: 45 C.F.R. 164.404(a)(2) further provides that a covered entity (DMHAS) 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).

Additional information considered in your determination:

Analysis:
Mitigation:

SECTION 1	
1. Is there a HIPPA Security/Privacy Rule violation? If Yes, then proceed to next question If No, then STOP here. No breach has occurred that requires notification.	Y / N
2. Was data secured (encrypted/unreadable, unusable or indecipherable to unauthorized users) properly destroyed in compliance with the requirements in the Breach Notification Rule? If Yes, then STOP here. No breach has occurred that requires notification. If No, then proceed to next question.	Y / N
3. Does this incident qualify as one of the following 3 exceptions (see below)? If Yes, then STOP here. No breach has occurred that requires notification. If No, then proceed to next section to work with the rest of the assessment to determine if the breach has a low probability that the PHI has been compromised to the extent that it would require notification.	Y / N
a. Good faith, unintentional acquisition, access or use of PHI by employee/workforce *Example: A billing employee receives and opens an email containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it.*	Y / N
b. Inadvertent disclosure to another person who is authorized to access PHI, and the information received is not further used or disclosed in a manner not permitted under the Privacy Rule. *Example: A physician who has authority to use or disclose protected health information at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital.*	Y / N
c. Recipient could not reasonably have retained the data *Example: A hospital, due to a lack of reasonable safeguards, sends a number of medical records to the wrong individuals. A few of the medical records are returned by the post office, unopened, as undeliverable. In these circumstances, the hospital can conclude that the improper addressees could not reasonably have retained the information.*	Y / N

If you did not hit a STOP above in Section 1, then go to Section 2 on the next page to determine whether the Protected Health Information was compromised to the extent that it would require notification.

SECTION 2 (circle all that apply in each subsection)		
I. PHI Form	• Verbal	1
	• Paper	2
	• Electronic	3
II. Recipient(s) of PHI	• Your Business Associate • Another Covered Entity • Internal Workforce	1
	• Wrong Payor (not the patient's) • Unauthorized family member • Non-covered entity	2
	• Media • Unknown/Lost/Stolen • Member of the general Public	3
III. Circumstances of release	• Unintentional disclosure of PHI	1
	• Intentional use/access w/o auth • Intentional disclosure w/o auth • Theft – Device targeted • Lost	2
	• Using false pretense to obtain or disclose • Obtained for personal gain/malicious intent • Hack • Theft – data targeted	3
IV. Disposition (What happened to the information after the initial disclosure)	• Information returned complete • Information properly destroyed and attested to	1
	• Information properly destroyed (unattested) • Electronically Deleted (unsure of backup status)	2
	• Sent to Media • Unable to retrieve • Unsure of disposition or location • High (suspicion of pending re-disclosure) • Extremely High (PHI already re-disclosed)	3
V. Additional Controls (Electronic disclosures only)	• Data Wiped • Information/Device Encrypted, but does not meet compliance with NIST Standards • Information Destroyed, but does not meet compliance with NIST Standards • Administrative Safeguards: Policy in place and adhered to	1
	• Password protected – password not compromised • Administrative Safeguards: Policy in place but not adhered to	2
	• Password protected – password not compromised • No Controls • Other _____	3
Section 2 - Total	***Add highest score from each subsection above and enter here:***	_____

SECTION 3

Analysis of factors to consider in determining the probability that the PHI has been compromised as a result of the impermissible use of disclosure

Comment on the following Factors

1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification.

(Consider the type of PHI involved, such as whether the disclosure involved information of a sensitive nature (e.g., credit cards; Social Security numbers; information that increases the risk of identity fraud; and clinical information, such as diagnosis, treatment plans, medication, medical history and test results). Consider the type of information disclosed to assess the probability that the PHI could be used by an unauthorized user in a manner adverse to the individual. If there are few, if any, direct identifiers in the PHI impermissibly disclosed or used, determine whether there is likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other available information.)

2. The unauthorized person who used the PHI or to whom the disclosure of PHI was made.

(Consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information (for example, if PHI is impermissibly disclosed to another entity obligated to abide by the HIPPA Privacy and Security Rules or to a federal agency obligated to comply with comparable regulations, there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity). If information impermissibly used or disclosed is not immediately identifiable, determine whether the unauthorized person who received the PHI has the ability to re-identify the information.

3. Whether the PHI was actually viewed or acquired or, alternatively, if only the opportunity existed for the information to be viewed or acquired.

(For example, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred or otherwise compromised, determination could be that the information was not actually acquired by an unauthorized individual even though the opportunity existed. If information was mailed to the wrong individual who opened the envelope and called the entity to say that she received the information in error, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.)

4. The extent to which the risk to the PHI bas been mitigated.

(Consider ability to obtain the recipient's satisfactory assurances that the information will not be further used or disclosed (through a written confidentiality agreement or similar means) or will be destroyed. Consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.)

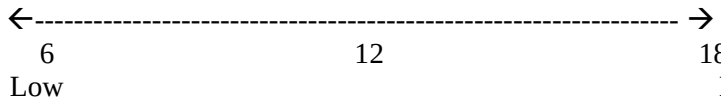
Probability of Compromise	Score
Low • **Information is not of a sensitive nature and is not likely to be used in a manner adverse to the individual or it is unlikely that information as disclosed could be re-identified.** • **The person who received the information has an obligation to protect it.** • **While the opportunity exists, it is not likely that the information was actually viewed or acquired.** • **There is documented confirmation from the recipient of the information that it was not copied, that it has been destroyed or returned to the facility and that any information s/he viewed and recalls will not be used or disclosed.**	**1**
Medium • **The information included sensitive clinical information but does not include SSN or other financial information that increases the risk of identity fraud.** • **The person who received the information has no obligation to protect it.** • **It is likely that the information was viewed.** • **The recipient of the information has memory of specific sensitive information. While the recipient may deny copying the information, states it has been destroyed and says s/he will not use or disclose the information, there is no written statement from the recipient and the PHI is not returned.**	**2**
High • **The information includes sensitive clinical and financial information.** • **The person who received the information has no obligation to protect it.** • **It is likely that the information was viewed.** • **There is no satisfactory assurance from the recipient that the information will not be used or disclosed and despite attempts to mitigate the impermissible use or disclosure there is risk of the information being used in a manner adverse to the individual.**	**3**

Please go to the next page to determine the Risk Score and whether the incident constitutes a reportable breach under HITECH.

SCORING

The scoring is meant to serve as a guide in your decision making and not designed to make the decision for you. There are a variety of factors and mitigations that may be involved in the incident that this tool cannot foresee or predict. All factors should be considered by the Incident Response Team when determining whether an incident constitutes a reportable breach under HITECH.

Total score from Section 2 (___) + Score from Section 3 (___) = Risk Sore:____



The range of scoring is 6-18. A low score of 6 does not necessarily mean you should not take any action but a high score of or near 18 could indicate either a need to notify or a need to take further actions.

After completing the assessment and scoring your responses do you feel the disclosure compromises the security and privacy of the PHI such that it poses a significant risk to the financial, reputational or other harm to the individual to the extent it would require a notification to the affected individuals?

NOTE: An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity demonstrates that there is a low probability that the PHI has been compromised.

If yes, the incident constitutes a reportable breach under HITECH.

Signature:_____ Date:_____
Compliance & Privacy Officer

Please refer back to the DMHAS Policy: **Breach Notification for Unsecured PHI Policy** to determine the next steps.

PHI Type	Date of Discovery	Date Breach Risk Assessment	Risk Assessment Score	Outcome Determination Date	Outcome

Key
B-Breach
P-Potential Breach
UD-Unauthorized Disclosure

Exhibit B

DMHAS Breach Notification for Unsecured PHI Policy
Health Information Privacy

Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information

Breach Affecting:

☐ 500 or More Individuals

☐ Less Than 500 Individuals

Report Type:

☐ Initial Breach Report

☐ Addendum to Previous Report

Section 1 – Covered Entity

Name of Covered Entity:

Address: **City:**

State: **Zip Code:**

Contact Name:

Contact Phone **Contact Email:**

Type of Covered Entity:

☐ Health Plan

☐ Health Care Provider

☐ Health Care Clearinghouse

Section 2 – Business Associate. Complete this section if breach occurred at or by a Business Associate.

Name of Business Associate:

Address: **City:**

State: **Zip Code:**

Business Associate Contact Name:

Business Associate Contact Phone **Business Associate Contact Email:**

Section 3 - Breach

Date(s) of Breach: **Date(s) of Discovery:**

MM/DD/YYYY MM/DD/YYYY

Approximate Number of Individuals Affected by the Breach:

Type of Breach: Please select the type of breach. If selecting the "Other" category, please describe the type of breach in more detail in the Description section below.

Select all that apply:

Theft	☐
Loss	☐
Improper Disposal	☐
Unauthorized Access	☐
Hacking/IT incident	☐
Other	☐
Unknown	☐

Location of Breached Information: Please select the location of the information at the time of the breach. If selecting the "Other" category, please describe the location of the information in more detail in the Description section below.

Select all that apply:

Laptop	☐
Desktop Computer	☐
Network Server	☐
E-mail	☐
Other Portable Electronic Device	☐
Electronic Medical Record	☐
Paper	☐
Other	☐

Type of Protected Health Information involved in the Breach: Please select the type of protected health information involved in the breach. If selecting an "Other" category, please describe the information in detail in the Description section below.

Select all that apply:

Demographic Information	☐
Financial Information	☐
Clinical Information	☐
Other	☐

Brief Description of the Breach: Please include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach:

Safeguards in Place Prior to Breach: Please indicate what protective measures were in place prior to the breach.

Select all that apply:

Firewalls	☐
Packet Filtering (router-based)	☐
Secure Browser Sessions	☐
Strong Authentication	☐
Encrypted Wireless	☐
Physical Security	☐
Logical Access Control	☐
Anti-Virus Software	☐
Intrusion Detection	☐
Biometrics	☐

Section 4 – Notice of Breach and Actions Taken

Date(s) Individual Notice Provided:
MM/DD/YYYY

Was Substitute Notice Required? ☐ Yes ☐ No

Was Medial Notice Required? ☐ Yes ☐ No

Actions Taken in Response to Breach: Please select the actions taken to respond to the breach. If selecting the "Other" category, please describe the actions taken in the section below.

Select all that apply:

Security and/or Privacy Safeguards	☐
Mitigation	☐
Sanctions	☐
Policies and Procedures	☐
Other	☐

Describe Other Actions Taken: Please describe in detail any actions taken following the breach in addition to those selected above.

Section 5 – Attestation

Responsible Senior Manager and Legal & Risk Services review and approval

I attest that I have reviewed and approve the above risk assessment and conclusion. To the best of my knowledge, the above information is accurate.

Name:_____ Date:_____
Agency Compliance & Privacy Officer

Name:_____ Date:_____
Agency Compliance Officer

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided in this form will be made publicly available by posting on the HHS web site pursuant to §13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to §13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.