

COUNTY OF MILWAUKEE  
Inter-Office Communication


**Date:** February 21, 2011  
**To:** Peggy West, Chair, Committee on Health and Human Needs  
**From:** Jerome J. Heer, Director of Audits  
**Subject:** Status Report – BHD Patient and Staff Safety Audit (File No. 10-390)

At its meeting on December 8, 2010, the Committee on Health and Human Needs voted 6-0 to receive and place our audit report, "System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County Behavioral Health Division," on file. Additionally, a follow-up report to be submitted for the March 2011 meeting cycle was requested.

Department of Health & Human Services (DHHS) management comments detailing its progress toward implementation of the recommendations are included in the attached status report for your review. DHHS management also provides information relating to the status of measures taken to address concerns over confidential patient information that appeared in newspaper articles in recent months. Copies of Behavioral Health Division Policies and Procedures in this area provided by management are also attached.

As noted in the status report, the majority of recommendations are being addressed and monitored by a combination of the Committee on Health and Human Needs, Community Advisory Board, Acute Executive Committee and the development of a work group to be comprised of a consortium of State and County representatives.

This status report is informational and we recommend it be received and placed on file.



Jerome J. Heer

JJH/PAG/cah

Attachments

cc: Health and Human Needs Committee Members  
Marvin Pratt, Interim County Executive  
Geri Lyday, Interim Director, Department of Health and Human Services  
Terrence Cooley, Chief of Staff, County Board Staff  
Jennifer Collins, Research Analyst, County Board Staff  
Jodi Mapp, Committee Clerk, County Board Staff

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title: System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD**

**File Number: 10-390**

**Page 1 of 10**

**Audit Date: October 2010**

**Status Report Date: February 14, 2011**

**Department: Behavioral Health Division**

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	
1. Continue monitoring and measuring compliance with key aspects of its corrective action plans related to the January 2010 and May 2010 CMS and DQA surveys.					Ongoing		Auditee: The Milwaukee County Behavioral Health Division Acute Inpatient Administration has continued to monitor and measure compliance with key aspects of its corrective action plans related to the January 2010 and May 2010 CMS surveys. To ensure corrective actions are achieved and sustained, progress toward improvement actions have continued to be monitored by the Acute Executive Committee. The frequency of ongoing monitoring will continue to be determined by the Acute Executive Team. The Director of Acute Inpatient Services provides progress updates to the Milwaukee County Behavioral Health Division Leadership Team and Director of Health and Human Services
2. Report results of its ongoing compliance measurements to the County Board Committee on Health and Human Services on a regular basis.					Ongoing		Auditee: The Director of Health and Human Services will continue to provide the Milwaukee County Board Committee on Health and Human Needs results of on-going compliance measurements. The frequency and duration of such updates will continue to be determined by the Chair of the Health and Human Needs Committee. For the last six months reports and updates have been provided monthly to the Health and Human Needs Committee

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title: System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD**

**File Number: 10-390**

**Audit Date: October 2010**

**Status Report Date: February 14, 2011**

**Page 2 of 10**

**Department: Behavioral Health Division**

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	
<p>3. Fashion a short-term strategy to address the small number of particularly aggressive/assaultive, difficult-to-place patients under the care of the BHD Adult Acute Inpatient hospital at any given time. Options considered should include:</p> <p>A. Re-configuring the present model of four mixed gender units (three general population and one for elderly/vulnerable patients) to include two single gender and one mixed gender units for the general population. While this would pose additional challenges to manage patient placements, it could help reduce the exposure of women with histories of sexual trauma to incidents of inappropriate sexual behaviors. The male-only unit would require enhanced security presence at an estimated additional cost of approximately \$175,000 annually.</p> <p>B. Allocating additional funds to place such patients at one of the two State Mental Health Institutions (Winnebago or Mendota). The additional cost of placing a patient in one of the state facilities for a year is approximately \$365,000.</p>	X		X		In process	X	<p>Auditee:</p> <p>BHD is relying on the expertise of its internal clinical team in consultation with qualified experts in the field and similar public acute inpatient psychiatric facilities. A BHD Work Group was appointed in April 2010, completed a <i>Preliminary Report</i> in May 2010 and embarked on a detailed study of the existing mixed-gender unit model. That study was completed and <i>Follow-Up Report</i> dated 12/01/2010 submitted to Interim BHD Administrator &amp; Interim Director HHS. The Report was presented to Milwaukee County Board Committee on HHN on 01/26/11. It will be presented to CAB and to Milwaukee County Supervisor Subcommittee on the BHD Facility. Recommendations for implementation are under consideration by Interim BHD Admin/Interim Director DHHS and BHD administrative and clinical leadership teams.</p> <p>High-risk patients who cannot be safely treated and managed within the BHD continuum of care shall continue to be evaluated on a case-by-case basis as to appropriateness for referral to one of the State Mental Health Institutes.</p>
					Ongoing		

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title: System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD**

**File Number: 10-390**

**Page 3 of 10**

**Audit Date: October 2010**

**Status Report Date: February 14, 2011**

**Department: Behavioral Health Division**

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	
C. Re-establishing a high-risk secure ward for particularly aggressive/assaultive patients. Estimating the additional cost of operating a high-risk secure ward would require detailed analysis but could easily reach \$2 million annually, plus additional start-up capital costs.	X		X		Ongoing	X	BHD is relying on the expertise of its internal clinical team in consultation with qualified experts in the field and similar public acute inpatient psychiatric facilities. A BHD Work Group was appointed in April 2010, completed a <i>Preliminary Report</i> in May 2010 and embarked on a detailed study of the existing mixed-gender unit model. That study was completed and <i>Follow-Up Report</i> dated 12/01/2010 submitted to Interim BHD Administrator & Interim Director HHS. The Report was presented to Milwaukee County Board Committee on HHN on 01/26/11. Will be presented to CAB on 02/23/10 and to Milwaukee County Supervisor Subcommittee on BHD Facility on 02/15/2011. Recommendations for implementation are under consideration by Interim BHD Admin/Interim Director DHHS and BHD administrative and clinical leadership teams.

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title: System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD**

**File Number: 10-390**

**Page 4 of 10**

**Audit Date: October 2010**

**Status Report Date: February 14, 2011**

**Department: Behavioral Health Division**

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	
4. Work with BHD's recently acquired management consulting firm and the Community Advisory Board for Mental Health to develop a long-term strategy for accommodating the treatment needs of particularly aggressive/assaultive, hard-to-place patients, with a goal of facilitating an appropriate alternative to extended periods of treatment in an acute inpatient facility.					In process	X	<p>Auditee: BHD is developing a work group specifically to address this small number of particularly aggressive patients at the Division. Because issues related to the care and treatment of these individuals cross multiple systems, BHD is facilitating the formation of a work group that includes representatives from the District Attorneys Office, Office of the Sheriff, State Forensic Unit, State of Wisconsin Division of Behavioral Health, State of Wisconsin Division of Long Term Care, BHD Administrative and Medical Staff and Milwaukee County Disability Services Department. Any potential solutions would likely require the involvement of representatives from each of these Divisions and would be best suited to identify long-term strategies and long term resources needed to address this complex issue.</p> <p>In late 2010, each member of the committee had been contacted and expressed a willingness to participate in this group. However, there has been a change in leadership at the state level and those individuals now need to be contacted to determine their willingness to participate. The BHD Administrator is expected to play an active role in the workgroup, but at this time, the position has not yet been filled.</p>

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title:** System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD

**File Number:** 10-390

**Audit Date:** October 2010

**Status Report Date:** February 14, 2011

**Page 5 of 10**

**Department:** Behavioral Health Division

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	
5. Staff the Acute Inpatient units with enough pool or 'floater' Certified Nursing Assistants to provide both sufficient coverage for heightened patient monitoring future (e.g., behavior observation checks and patient escorts to court appearances), as well as a relief factor for staff breaks. The county Executive's 2011 Proposed Budget includes 18 FTE CNA positions, which believe is adequate for these purposes.					Ongoing		<p><b>Auditee:</b> Unit acuity and patient safety concerns continue to be assessed/evaluated daily at the noon safety meeting. The status of all patients on one-to-one observation monitoring is also reviewed at this meeting. This is important to maintain patient safety but also to monitor effective utilization and distribution of nursing staff. In preparation for the hiring of the 2011 additional CNA positions, we have internally redistributed some of our existing CNA positions. This was an effort to correct some structural deficits in unit staff numbers, as well as, promote consistency in staffing. The first group of new 2011 CNAs is being recruited for a March orientation class. We will continue to hire the new CNAs in groups of ten to twelve to allow optimal orientation and adequate management oversight of performance.</p>
6. Continue its efforts to pursue accreditation from The Joint Commission, and prepare a report for the June 2011 meeting of the County Board Health and Human Needs Committee on progress toward, and any impediments to, achieving accreditation in 2012.					Ongoing		<p><b>Auditee:</b> The Milwaukee County Department of Health and Human Services has retained the services of the consulting firm "Critical Management Solutions" to assist the Division in working towards the goal of Joint Commission accreditation. In addition, there is \$48,830 dedicated towards maintaining this initiative in the 2011 Budget. Additional positions are approved and being recruited to achieve Joint Commission accreditation. An initial visit to determine survey readiness was completed the last quarter of 2010. The BHD leadership team's goal is to attain Joint Commission Accreditation during calendar year 2012. The Joint Accreditation Consulting Group is scheduled to be back at BHD in March 2011.</p>

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title: System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD**

**File Number: 10-390**

**Audit Date: October 2010**

**Status Report Date: February 14, 2011**

**Page 6 of 10**

**Department: Behavioral Health Division**

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	
7. Provide a report to the County Board Health and Human Needs Committee for its December 2010 meeting detailing the status of compliance with each of the recommendations contained in the June 2010 security review conducted by the Milwaukee County Sheriff's Office.	X		X		Yes	No	Auditee: A report was provided to the County Health and Human Needs Committee in December 2010 regarding compliance with the 2010 security review. BHD has implemented the majority of the recommendations from the report from the Office of Sheriff, to advance the safety and security of the facility.
8. Install electronic monitoring devices on each inpatient unit to record the frequency with which security staff assigned as a rover among the units is completing assigned rounds	X		X		Completed		Auditee: Each unit is now currently equipped with an electronic touch pad at all the nurses stations and at the end of the unit corridor. The contracted security company has purchased an additional wand for the rover, to use on a daily basis. The data is downloaded and reviewed by the security supervisor in conjunction with BHD Operations and Administration. Since the audit review was conducted, security cameras were installed on the Acute Adult units. These cameras cannot record data due to state and federal regulations but are viewed live by security personnel. This supplements the rover tours and has resulted in quicker responses in potential code situations.  Each security guard assigned as a rover walks onto each unit from the main entrance or from the nurses station back entrance and performs the following activities: <ul style="list-style-type: none"> <li>▪ Checks in with nursing staff regarding any "potential hot spots/areas;"</li> <li>▪ Walks down both hallways;</li> <li>▪ Checks that the community bathroom is locked along with other required locked doors;</li> <li>▪ Observes environment for any concerns and stands by while nursing staff assess the situation and take action as directed.</li> </ul>

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title:** System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD

**File Number:** 10-390

**Audit Date:** October 2010

**Status Report Date:** February 14, 2011

**Page 7 of 10**

**Department:** Behavioral Health Division

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	
							<p>Frequently, the rover is called to stand by on one unit and before that assignment is over they are called to another unit for a different stand-by situation. This makes setting a required number of tours per hour difficult as it may vacillate greatly from day to day due to other code situations and the requested stand-by events. Security staff completed an uninterrupted rover tour of all 5 units on October 20, 2010 to determine what the shortest duration for a tour might be. One uninterrupted tour took 30 minutes. This test did not include any time for information exchange with nursing staff, which could run 2-5 minutes. Thus, the duration of each tour will continue to be contingent upon how much must be communicated regarding "hot spots" and if the security guard needs to linger in any location to determine if there is cause for concern over anything observed. Using an estimate of 40 minutes per tour, with the minimum 2 minutes of check-in time at each unit (10 minutes total), and assuming each shift will have between 10 and 15 stand-by requests (average 15 minutes each), 7 tours per shift will continue to be a realistic <u>minimum</u> requirement.</p>



**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title: System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD**

**File Number: 10-390**

**Page 8 of 10**

**Audit Date: October 2010**

**Status Report Date: February 14, 2011**

**Department: Behavioral Health Division**

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	

The request was also made by Supervisor West to review the status of measures taken to address concerns over confidential Patient information that appeared in newspaper articles in recent months.

Training related to disclosure of protected Patient information is provided to all employees at their orientation. There are also annual training updates that occur yearly that focus on confidentiality issues. Any confidentiality violations are reported to the BHD privacy officer. At BHD the privacy officer is the Director of Medical Records. Upon notification, each situation is reviewed to determine an appropriate response according to the attached policies. Violations that rise to the level of a disciplinary offense are referred on to individual program areas for review and appropriate follow up.

Milwaukee County Corporation Council as well as the BHD privacy officer reviewed the disclosure incident that is being referred to. Each independently found that the disclosure was allowable under current confidentiality laws given the circumstances in which it occurred. Please see the following excerpt from an email from Corp. Council Attorney Jorgensen. The situation being described is where a BHD RN read a victim's letter in open court. A BHD Patient assaulted this RN and was initially charged with a criminal offense. The Case was ultimately dismissed because the individual was found, not competent to stand trial.

*"There is no reason to assume there was a violation of the HIPAA privacy rule by BHD staff. Under 45 CFR 164.502(j)(2), a covered entity does not violate the rule if*

*a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official [which, under the HIPAA definitions, includes prosecutors], provided that:*

- (i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and*
- (ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).*

*The information listed in the cross-referenced rule is:*

- (A) Name and address;*
- (B) Date and place of birth;*
- (C) Social security number;*
- (D) ABO blood type and rh factor;*
- (E) Type of injury;*

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title:** System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD

**File Number:** 10-390

Page 9 of 10

**Audit Date:** October 2010

**Status Report Date:** February 14, 2011

**Department:** Behavioral Health Division

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

There are related exceptions under 45 CFR 164.512(f) that permit disclosure "for law enforcement purposes". In particular, subsec. (5):

(5) Permitted disclosure: Crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

and subsec. (1)(c), which permits disclosure in response to an "authorized investigative demand", a term sufficiently broad to encompass a demand from a DA in the course of a criminal prosecution:

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

In addition to the HIPAA privacy rule, there are, of course, Wis. Stat. s. 51.30 and the implementing regulations, ch. HFS 92, Wis. Adm. Code, which predate HIPAA by many years and are often more stringent (and, to that extent, preempt HIPAA). Sec. 51.30(4)(b)19 permits disclosure without informed consent to report a crime committed in the facility:

19. To state and local law enforcement agencies for the purpose of reporting an apparent crime committed on the premises of an inpatient treatment facility or nursing home, if the facility or home has treatment records subject to this section, or observed by staff or agents of any such facility or nursing home. Information released under this subdivision is limited to identifying information that may be released under subd. 16. and information related to the apparent crime.

**STATUS OF IMPLEMENTING DEPARTMENT OF AUDIT REPORT RECOMMENDATIONS**

**Audit Title: System Changes are Needed to Help Ensure Patient and Staff Safety at the Milwaukee County BHD**

**File Number: 10-390**

**Page 10 of 10**

**Audit Date: October 2010**

**Status Report Date: February 14, 2011**

**Department: Behavioral Health Division**

Number & Recommendation	Deadlines Established		Deadlines Achieved		Implementation Status		Comments
	Yes	No	Yes	No	Completed	Further Action Required	

*State law is less generous than HIPAA with regard to disclosure of treatment record information for any purpose beyond the initial "reporting" of an "apparent crime", such as investigation and prosecution. Logically, the authority to disclose information to report a crime suggests that information could be disclosed, on a need-to-know basis, to investigate and prosecute that crime, but no express provision of state laws allows that. In fact state law is quite restrictive, requiring, for instance, an order or subpoena signed by a judge more most disclosures to law enforcement.*

*I look forward to discussing this with you.*

*John"*

The relevant BHD Policies are as follows and are being sent via email as attachments.

1. Incident Reporting
2. Confidentiality Procedures- Client Information
3. Confidentiality Breach- Notification

(7)

<b>POLICY &amp; PROCEDURE</b>  <b>MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</b>  <b>DEPARTMENT: ADMINISTRATION</b>	<b>DATE ISSUED</b> —09/23/05 <i>9/20/02</i>	<b>SECTION:</b>	<b>POLICY #</b>	<b>PAGE</b> 1 of 8
	<b>DATES REVISED</b> 03/01/93 03/31/94 02/27/97 09/23/05	<b>SUBJECT:</b>  <b>INCIDENT REPORTING</b>		

**Policy:** It is the policy of the Milwaukee County Behavioral Health Division that significant incidents and exposure to risk will be reported, monitored, and investigated if indicated. Serious incidents involving patients/residents, staff, students, volunteers, security or contracted personnel, and visitors will be reported on an Incident/Risk Management Report Form. Specific policies and reporting procedures will be followed for each type of incident listed in this policy. Staff are expected to immediately notify their supervisor about serious incidents including allegations of caregiver misconduct, possible patient/resident injuries of unknown origin, death, serious injury and physical or sexual assault.

**A. Procedure for Incident Reporting:**

1. In the event of the occurrence of any of the events listed below, an Incident/Risk Management Report Form (4310-latest draft) will be completed. The report will be completed by:

- the employee(s) or staff involved in the incident,
- or
- the staff who observed the incident,
- or
- in the situation where no staff are present, by the staff who interviewed the patient/resident, student, volunteer, visitor or security/contract personnel involved.

**2. Reportable Incidents**

**ADVERSE DRUG REACTION** - A suspected or unintended physical and/or allergic reaction to a medication when prescribed and used in an approved manner. A message should be left on the BHD pharmacy hotline 454-4262. Consult the Adverse Drug Reactions and Medication Variances Policy MS 5.2.6 for additional information and reporting requirements.

**MEDICATION VARIANCE CAUSING HARM** - Any medication action that is not consistent with routine medical operation or routine care that causes patient harm. This includes errors related to dose, time of administration or ingestion, route of administration, type of medication, incorrect transcription, packaging, etc. For medication variance causing unintended physical consequences, or harm to the patient, complete both the Incident/Risk Management Report Form and the Medication Variance Form (Photocopy #472-1). For medication variance, which does not cause physical harm, only complete the Medication Variance Report Form. Consult the Adverse Drug Reactions and Medication Variances Policy MS 5.2.6 for additional information and reporting requirements.

<p style="text-align: center;">POLICY &amp; PROCEDURE</p> <p style="text-align: center;">MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</p>	<p style="text-align: center;">SUBJECT: INCIDENT REPORTING</p>	<p style="text-align: center;">Page 2 of 8</p>
--	--	--

**CAREGIVER MISCONDUCT ALLEGATION** - Report any observed or reported potential caregiver misconduct. Caregiver misconduct includes physical, sexual, or verbal abuse. It includes staff behavior such as harassment, intimidation, threats, humiliation, frightening, and forcing medications. It includes allegations of theft or misappropriation of a patient or resident's funds by a caregiver. **Your supervisor or designee or if unavailable any individual who is a supervisor must be notified immediately.** Consult BHD Caregiver Misconduct Policy.

**CODE 4/MEDICAL EMERGENCY** - Serious medical emergencies resulting in a "Code 4" being called. For a Code 4 event consult Medical/Nursing Staff Policy 6.2.1 for additional reporting requirements.

**CONFIDENTIALITY BREACH** – Information about a patient/resident that identifies the patient/resident, which is intentionally or unintentionally released without the patient or resident's consent (or parent, guardian, power of attorney consent), is a breach of confidentiality. Unless there is a legal exception, per federal regulations, this breach must be reported. Legal exceptions allowing release of patient/resident's medical information without consent are detailed in chapter 51.30 of the state statutes and federal Health Insurance Portability and Accountability Act (HIPAA) regulations. Before reporting a confidentiality breach employees should consult with supervisor/designee and/or Medical Records Director/Privacy Officer.

**DEATH** - File an Incident/Risk Management report for all deaths. Refer to Medical Record policy MRD-003/Medical Staff Policy 6.4.8 Procedure Following a Patient Death.

**EXPOSURE TO INFECTION** - Unprotected contact with a communicable organism's known means of transmission. Report exposures such as needle sticks, human bites, contact with blood and body fluids on non-intact skin (mouth, eyes, cuts, etc.) and contacts with individuals diagnosed with active tuberculosis.

Employees who are exposed, **must notify their supervisor**, and in addition to the incident risk management report, complete the Milwaukee County Accident/Loss Report Form (#3676-1). The exposed staff should send the original Accident/Loss Report Form to BHD Human Resources and a copy to the supervisor/designee.

**FALL** - An individual is seen falling or reports having fallen

**FIRE** - Report any fires or attempts at setting fires. The sheriff should be called for arson. A fire alarm incident report may have to be completed by the supervisor (#f3800). Fires which involve evacuation from the facility must be reported to the state.

<p style="text-align: center;"><b>POLICY &amp; PROCEDURE</b></p> <p style="text-align: center;"><b>MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</b></p>	<p style="text-align: center;"><b>SUBJECT: INCIDENT REPORTING</b></p>	<p style="text-align: center;">Page 3 of 8</p>
--	---	--

**HAZARDOUS MATERIALS/ENVIRONMENTAL CONTAMINANT** -Exposure to hazardous chemical substances, materials, or pollutants, which may be inhaled, ingested, or absorbed through the skin.

Employees who are exposed, **must notify their supervisor**, and in addition to the incident risk management report, complete the Milwaukee County Accident/Loss Report Form (#3676-1). The exposed staff should send the original Accident/Loss Report Form to BHD Human Resources and a copy to the supervisor/designee before the end of their shift.

**INJURY** - An injury for which medical or nursing attention is required. **Patient/resident injuries without any known origin or source should be documented as unknown and reported to your supervisor/designee immediately.** Examples of injuries include: accidents, self-injuries, and injuries during seclusion and restraint. For serious injuries consult Medical staff policy 6.4.8-Sentinel Events. For injuries of unknown origin or source consult BHD Caregiver Misconduct Policy.

Employees who are injured, **must notify their supervisor**, and in addition to the incident risk management report, complete the Milwaukee County Accident/Loss Report Form (#3676-1). **Staff should send the original Accident/Loss Report Form to BHD Human Resources and a copy to the supervisor/designee before the end of their shift.**

**MEDICAL DEVICE/EQUIPMENT FAILURE** - Failure of equipment involved with providing patient/resident care that results in injury or risk of injury.

**MISSING PROPERTY/MONEY** - Report missing personal property, valuables, and money. The supervisor, AR, Administrator, medical staff, or designee should notify the sheriff, if theft of patient/resident valuables or county property is suspected. Employees, visitors, security or contract personnel, students, or volunteers should contact the sheriff on their own if theft of personal property is suspected. **If a patient/resident, family member or guardian alleges that a caregiver took an item belonging to a patient/resident your supervisor should be notified immediately.** Consult BHD Caregiver Misconduct Policy.

**PHYSICAL ASSAULT** - Assaults in which an individual causes bodily harm such as when striking, hitting, kicking, biting, spiting, grabbing another, etc. For allegations of physical assault the sheriff/police should be notified by the supervisor, AR, Administrator, medical staff, or designee. For information regarding reporting patient assaults consult Medical Staff policy 6.4.7 Prosecution of Patients for Presumptively Criminal Acts.

**PROPERTY DAMAGE/LOSS** - Report damage of Milwaukee County property and personal property. Significant, purposeful damage should be reported to the sheriff by the supervisor, AR, Administrator, medical staff, or designee.

<p style="text-align: center;"><b>POLICY &amp; PROCEDURE</b></p> <p style="text-align: center;"><b>MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</b></p>	<p style="text-align: center;"><b>SUBJECT: INCIDENT REPORTING</b></p>	<p style="text-align: center;">Page 4 of 8</p>
--	---	--

**SEXUAL CONTACT-** Physical contact of a sexual nature between patients/residents or between a patient/resident and a staff member, visitor, volunteer, or student. For dealing with sexual contact between patients/residents consult Medical/Nursing Staff policy 6.4.6. The supervisor, AR, Administrator, medical staff, or designee should notify the sheriff if nonconsensual sexual contact is alleged. For staff and patient/resident contact consult BHD staff/patient relationship policy BHD 129E and BHD Caregiver Misconduct policy.

**SUICIDE ATTEMPT/SELF INJURY -** All serious attempts at self harm, including self-injurious behavior such as cutting or burning self on purpose, overdose etc. Consult Medical Staff policy 6.4.9 Post Suicide or Suicide Attempt Evaluation Process.

**UNAUTHORIZED ABSENCE -** All elopements from locked units must be reported unless the patient/resident returns immediately. All elopements while the patient/resident is being escorted must be reported unless the patient returns immediately. Failure of a patient/resident to return from off ward privileges, or a pass, within thirty minutes of the expected time must be reported. For unlocked units, failure of a resident to return to the unit when the resident is incapable or unlikely of returning on his/her own must be reported.

Consult BHD Policy 101 S and Medical Staff Policy 6.4.4 to determine if a Missing/UA Request Form must be completed (#4399) and if the sheriff or other law enforcement agencies must be notified by the supervisor, AR, Administrator, medical staff, or designee.

**OTHER-** Report other incidents in which there was serious risk to patients/residents, staff, volunteers, students, and visitors. Consult with your supervisor **before** completing this form to determine if it is appropriate to use.

3. The Incident/Risk Management Report Form **must** be completed before the end of the employee's shift or work period and before leaving the premises. The supervisor or designee should receive the report as well as other required reports (e.g. employee accident/loss report) by the end of the shift. If the supervisor or designee is unavailable the report should be put in the supervisor's mailbox or designated mailbox with voice mails or e-mail messages alerting the supervisor/designee and program administrator/department head/designee. For Sentinel Events the report should be given to the program administrator or administrator on call if the supervisor is unavailable.

4. The supervisor or designee, and if unavailable, the program administrator or administrator on call must be **immediately (within 15 minutes)** contacted for sentinel, or high risk events (high likelihood of serious adverse outcome). Incidents that involve death, fires, explosions, serious injuries and assaults, substantial damage, or property loss, must be reported **immediately**. Allegations of caregiver misconduct and patient/resident injuries of unknown origin must be reported **immediately**.

<p style="text-align: center;"><b>POLICY &amp; PROCEDURE</b></p> <p style="text-align: center;"><b>MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</b></p>	<p style="text-align: center;"><b>SUBJECT: INCIDENT REPORTING</b></p>	<p style="text-align: center;">Page 5 of 8</p>
--	---	--

**B. Supervisor Responsibilities**

1. Upon receiving a report of an incident the supervisor/designee will do the following:
  - a. Notify the program administrator or administrator on call immediately for sentinel or high risk events, for caregiver misconduct allegations, and for patient/resident injuries of unknown origin.
  - b. Make sure that staff notify the physician/ MOD, RN, Attending psychologist (if during regular working hours), QMRP (if during regular working hours), Nursing Program Coordinator (if during regular hours), and Administrative Resource (if during non-regular hours), assigned to unit or program, if they have not already done so for the following: patient/resident physical injuries, patient/resident sexual contact, code four, patient/resident exposure to infection, allegations of caregiver misconduct, unauthorized absences, suicide attempts and deaths.
  - c. Make sure that staff notify the physician/ MOD, and RN, and call pharmacy hotline for adverse drug reactions, and notify the physician/MOD and RN, and complete the medication Variance Report Form for medication errors causing harm
  - d. Notify sheriff/police for the following: physical assaults, sexual contact involving non-consenting individuals, allegations of theft, fires, and destruction of patient/resident or county property, and for unauthorized absences and elopements for involuntary patients/residents and patients/residents on police holds. The supervisor may designate staff to call the sheriff.
  - e. Notify the patient/resident's guardian, parent, or power of attorney for health care for significant injuries, code 4/medical emergencies, deaths, sexual contact (if a juvenile), sexual assaults, allegations of caregiver misconduct, sheriff/police notification, and unauthorized absence. Document notification in a progress note in the patient/resident's medical record.
  - f. Consult the Sentinel Event Policy (Medical staff policy 6.4.8) for additional supervisory staff to contact if there is a sentinel event.
  - g. Inspect the report for completeness, and make additions as needed to the notification section.
2. For allegations of caregiver misconduct or possible patient/resident injuries of unknown origin., the supervisor should list the administrator called under "notifications", and check the box indicating the administrator/designee was notified.
3. The supervisor/designee should document his/her review of the incident including any actions taken and any investigation initiated. Referrals to the patient/resident's treatment team should be documented. For sentinel, or high risk events (high likelihood of serious adverse outcome), and incidents that involve death, fires, explosions, serious injuries and assaults, substantial damage or property loss, elopements



<p style="text-align: center;">POLICY &amp; PROCEDURE</p> <p style="text-align: center;">MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</p>	<p style="text-align: center;">SUBJECT: INCIDENT REPORTING</p>	<p style="text-align: center;">Page 6 of 8</p>
--	--	--

from locked units or while patient/resident is being escorted, only the supervisor's initial investigation should be reported on the incident/risk management reporting form. Later investigations should be documented as a written report. Allegations of caregiver misconduct and patient/resident injuries of unknown origin require a separate investigation, which is reported on a separate form (see Caregiver Misconduct: Reporting and Investing Caregiver Misconduct and Injuries of Unknown Origin). Sentinel events will also be investigated by members of the Critical Incident committee who will make a determination of the level of investigation required.

**4. The Incident/Risk Management Report Form (original and yellow copy) should be given by the supervisor to the Program Administrator or Department head or designee as soon as the initial investigation is completed.**

**C. Follow Up Review**

1. The program administrator, department head, or designee must review the incident within three working days of receiving the Incident/Risk Management Report Form. She or he must make a decision as to whether follow up review is needed, initial the form, and send the original and any attachments to the Quality Management Department. She or he should never delay sending the form because of additional review by the program and/or department.
2. A written follow up report should be completed whenever the program administrator/department head/designee appoints an investigator for further review. **Exception: For allegations of caregiver misconduct and injuries of unknown origin the investigation must be started immediately. Review the investigation procedure under the BHD Reporting and Investigation of Caregiver Misconduct Policy.**
3. The program administrator/department head/designee should establish timelines for completing and reporting on the follow up investigation unless further investigation will be performed through the Critical Incident committee. For investigations of allegations of caregiver misconduct the report must be received by the state within seven calendar days of the incident. If the reviewer is unable to complete the report within the timeline, Quality Management and the program administrator/department head/designee should be notified and a new timeline developed.
4. When reviewing an incident and determining the level of investigation the program administrator/department head/designee should consider the level of severity, level of risk, and outcomes. The thoroughness of the investigation, amount of follow up action, and need for corrective action should be based on the severity of the incident.
5. For sentinel, or high risk events (high likelihood of serious adverse outcome), and incidents that involve death, fires, explosions, serious injuries and assaults, and substantial damage or property loss, the Critical Incident committee will be involved with the program or department in the investigation.

<p style="text-align: center;"><b>POLICY &amp; PROCEDURE</b></p> <p style="text-align: center;"><b>MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</b></p>	<p style="text-align: center;"><b>SUBJECT: INCIDENT REPORTING</b></p>	<p style="text-align: center;">Page 7 of 8</p>
--	---	--

#### **D. Investigative Process**

1. It is the investigator's responsibility to perform an adequate investigation by collecting sufficient information to determine the need for follow up actions and to provide justification for corrective action. All staff at MCBHD are required to participate if needed in the investigative process. Refusal to participate is grounds for disciplinary action.

#### **2. Investigative Procedure:**

a. The first step in the investigation process is to review the incident report when it is received to ensure that it is correctly completed, signed and dated, and that supporting materials are included.

b. The second step of the investigation is to review the incident as described in the report and to review any included materials. Part of the review will usually include discussing the incident with the individual completing the report. Other outcomes since the incident report was filed should also be reviewed.

c. When the investigation is determined to require more depth the specific individuals who are listed as witnesses should be interviewed as soon as possible. The investigator should use signed written statements from witnesses for investigations when there may be significant legal or disciplinary outcomes. The investigator may write down an oral statement and have the witness sign it. It is important to only include directly observed facts and not opinion or hearsay in witness statements.

d. After the initial investigation is completed the investigator must determine the need to expand the investigation. More information should be collected if it is needed for fact finding, or to determine the types of actions to be recommended. This may include interviewing additional witnesses and reviewing additional supporting documents.

2. Referrals for further investigation and recommendations for corrective action should be based on the severity of the incident and the need to ensure risk reduction. For example adverse drug reactions will require referral to the Pharmacy and Therapeutics committee. Recommendations for corrective action may include mandatory education or changes in employee practice. The program administrator/department head/designee should review the findings to determine if further action is warranted.

3. The investigator should complete a written follow up report. The reviewer should provide adequate documentation to justify whether or not follow up action is needed. A brief reason should be noted for making a referral. If substantive corrective action is being recommended (for example an educational

<p style="text-align: center;"><b>POLICY &amp; PROCEDURE</b></p> <p style="text-align: center;"><b>MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION</b></p>	<p style="text-align: center;"><b>SUBJECT: INCIDENT REPORTING</b></p>	<p style="text-align: center;">Page 8 of 8</p>
--	---	--

inservice for all employees in the program), the reviewer should provide a rational in terms of reducing risk, ensuring practice standards are met, etc.

4. The report should be sent to the program administrator/department head/designee. She or he is responsible for forwarding the investigative report to Quality Management and for making referrals for further investigation.

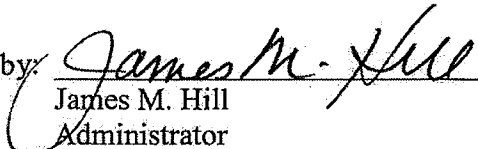
**D. Quality Assurance Department**

Staff in the Quality Assurance Department will be responsible for notifying appropriate administrators and committee chairpersons, making recommendations for additional investigation, maintaining a database of incidents, and compiling quantitative reports on incidents.

**List of Policies and Procedures referred to:**

- Adverse Drug Reactions and Medication Variances MS 5.2.6
- Caregiver Misconduct: Reporting and Investing Caregiver Misconduct and Injuries of Unknown Origin
- Code 4 MS/N 6.2.1
- Health Insurance Portability and Accountability Act (HIPAA)
- Line of Duty Injury or Illness
- Missing/UA Patients MS 6.4.4 & BHD 101S
- Patient/Staff Relationships BHD 129E
- Post Suicide or Suicide Attempt Evaluation Process MS 6.4.9
- Procedure Following a Patient Death MS 6.4.8 & MRD 003
- Prosecution of Patients for Presumptively Criminal Acts MS 6.4.7
- Sentinel Event MS 6.4.8
- Sexual Contact Between Patients MS/N 6.4.6
- Sexual Harassment Policy
- State statute Chapter 51.30
- Workplace Violence Prevention Policy

prepared by: Tim Wiedel Ph.D. and members of the ad hoc Incident Reporting Committee

Approved by:   
 James M. Hill  
 Administrator  
 September 27, 2005

POLICY AND PROCEDURE  MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION	DATE ISSUED: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY		
	DATE REVIEWED* / REVISED:	SECTION:  HITECH	POLICY NUMBER:  3005	PAGE(S)  1 of 9
INFORMATION MANAGEMENT				

**Purpose:** To provide guidance for breach notification by covered entities when impermissible or unauthorized access, acquisition, use and/or disclosure of the Milwaukee County Behavioral Health Division's (MCBHD or BHD) patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The rule is effective September 24, 2009 with full compliance required by February 22, 2010.<sup>1</sup> (See Attachment 1 for Monetary Penalties.)

**Background:**

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

NOTE: For definitions, please see page 5.

**Policy Statement/ Procedures:**

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 Behavioral Health Division (BHD), or, by exercising reasonable diligence would have been known to BHD (includes breaches by the organization's business associates). BHD 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 the organization (See Attachment 2). Following the discovery of a potential breach, BHD 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 BHD to have been, accessed, acquired, used, or disclosed as a result of the breach. BHD shall also begin the process of determining what external notifications are required or should be made (e.g.,

<sup>1</sup> 16 CFR Part 318 Available at: <http://www.ftc.gov/os/2009/08/R911002hbn.pdf>.

POLICY & PROCEDURE	DATE: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY	PAGE(S) NUMBER 2 of 9
-----------------------	----------------	--	-----------------------------

Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. Breach Investigation: The BHD HIPAA Privacy Officer or Security Officer as appropriate, are appointed to administer or delegate the investigation of the breach. The assigned investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others at BHD as appropriate (e.g., administration, human resources, risk management, legal counsel, etc.) The Privacy and/or Security Officer 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.<sup>2</sup>
  
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 incidental 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, the organization 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.<sup>3</sup> (See Attachment 3) BHD shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization 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, BHD will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:
  - A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
  - B. The type and amount of PHI involved.
  - C. The potential for significant risk of financial, reputation, or other harm.
  
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 BHD or the business associate involved. It is the responsibility of BHD to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.
  
5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official indicates to us that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, BHD shall:

<sup>2</sup> 45 CFR §164.530(j)(2).

<sup>3</sup> BHD may choose to make the decision to notify patients of a breach even after completion of the risk assessment indicates that there is no requirement to do so under ARRA/HITECH.

POLICY & PROCEDURE	DATE: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY	PAGE(S) NUMBER 3 of 9
-----------------------	----------------	--	-----------------------------

- A. If the statement is in writing and specifies the time for which a delay is required, BHD shall 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 identify 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.<sup>4</sup>
6. Content of the Notice: The notice shall be written in plain language and must contain the following information(See Attachment 4):
- 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 BHD 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 (See Attachment 5):
- 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 the BHD 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.

<sup>4</sup> 45 CFR § 164.412.

POLICY & PROCEDURE	DATE: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY	PAGE(S) NUMBER 4 of 9
--------------------	----------------	---	-----------------------------

- 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 the organization's website, or a conspicuous notice in a major print or broadcast media in the Milwaukee geographic area 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.
        - 3. If BHD 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.
          - B. 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. (See Attachment 6)
          - C. 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.<sup>5</sup>(See Attachment 7)
            - 1. For breaches involving 500 or more individuals, BHD shall notify the Secretary of HHS as instructed at [www.hhs.gov](http://www.hhs.gov) at the same time notice is made to the individuals.
            - 2. For breaches involving less than 500 individuals, BHD will maintain a log of the breaches and annually submit the log to the Secretary of 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](http://www.hhs.gov).<sup>6</sup>
8. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the BHD Privacy and Security Officers will ensure that a process is maintained to record or log all breaches of unsecured PHI regardless of the number of patients affected.<sup>7</sup> The following information should be collected/logged for each breach (See Attachment 8 sample Breach Notification Log):
  - A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
  - B. 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, etc.).

<sup>5</sup> Note: If the breach involves "secured" PHI, no notification needs to be made to HHS.

<sup>6</sup> For calendar year 2009, BHD is required to submit information to the HHS secretary for breaches occurring after the September 23, 2009 effective implementation date.

<sup>7</sup> BHD shall delegate this responsibility to one individual (e.g., Privacy Officer).

POLICY & PROCEDURE	DATE: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY	PAGE(S) NUMBER 5 of 9
-----------------------	----------------	--	-----------------------------

- C. A description of the action taken with regard to notification of patients regarding the breach.
- D. Resolution steps taken to mitigate the breach and prevent future occurrences.

9. Business Associate Responsibilities: A business associate (BA) of BHD 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 BHD 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.<sup>8</sup> The BA shall provide BHD with any other available information that BHD 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, BHD 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).

10. Workforce Training: BHD 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 the BHD.

11. Complaints: BHD must provide a process for individuals to make complaints concerning the BHD's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the BHD's breach notification processes.<sup>9</sup>

12. Sanctions: BHD must apply progressive discipline based on Civil Service Work against members of its workforce who fail to comply with privacy policies and procedures.

13. Retaliation/Waiver: BHD 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. BHD may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

### Definitions:

<sup>8</sup> Business associate responsibility under ARRA/HITECH for breach notification should be included in BHD's business associate agreement (BAA) with the associate (See [www.hipaacow.org](http://www.hipaacow.org) for BAA information).

<sup>9</sup> The BHD may want to consider adding this right to complaint about the breach notification process to their Notice of Privacy Practices.



POLICY & PROCEDURE	DATE: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY	PAGE(S) NUMBER 6 of 9
-----------------------	----------------	--	-----------------------------

Access: The ability or means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.<sup>10</sup>

Breach: The acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputation, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

Breach excludes:

1. 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 Privacy Rule.
2. 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.
3. A disclosure of PHI where a CE or BA 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.<sup>11</sup>

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.<sup>12</sup>

Disclosure: The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.<sup>13</sup> An incidental disclosure is when in spite of our best efforts a breach occurs. An example might be that a maintenance worker can view the names on patient charts while changing light bulbs in the file room, or overhears a conversation regarding patient care even though the treatment staff are talking quietly to protect privacy.

Individually Identifiable Health Information: 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 the 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.<sup>14</sup>

<sup>10</sup> 45 CFR § 164.304.

<sup>11</sup> ARRA/HITECH Title XIII Section 13400; §164.402,

<sup>12</sup> 45 CFR § 160.103.

<sup>13</sup> 45 CFR § 160.103.

<sup>14</sup> 45 CFR § 164.503.

POLICY & PROCEDURE	DATE: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY	PAGE(S) NUMBER 7 of 9
-----------------------	----------------	--	-----------------------------

Law Enforcement Official: Any officer or employee of an 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.<sup>15</sup>

Organization: For the purposes of this policy, the term "BHD" shall mean the covered entity to which the policy and breach notification apply.

Protected Health Information (PHI): Individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.<sup>16</sup>

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.<sup>17</sup> The following encryption processes meet this standard.
  - A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
  - B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
  - A. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
  - B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI

<sup>15</sup> 45 CFR § 164.103.

<sup>16</sup> 45 CFR § 164.503.

<sup>17</sup> 45 CFR Parts 160 and 164; Final Rules Issued 8/19/09.

POLICY & PROCEDURE	DATE: 10/09	SUBJECT: BREACH NOTIFICATION-PROTECTED HEALTH INFORMATION POLICY	PAGE(S) NUMBER 8 of 9
-----------------------	----------------	--	-----------------------------

cannot be retrieved.<sup>18</sup>

**Workforce:** Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.<sup>19</sup>

**Applicable Federal/State Regulations:**

- ARRA Title XIII Section 13402 – Notification in the Case of Breach
- FTC Breach Notification Rules - 16 CFR Part 318
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules
- WI § 134.98 – Notice of Unauthorized Acquisition of Personal Information (Note: Not applicable to Covered Entities Under HIPAA).
- WI 51.30 HFS 92

**Attachments:**

- Breach Penalties (Attachment 1)
- Examples of Breaches of Unsecured Protected Health Information (Attachment 2)
- Risk Assessment Analysis Tool (Attachment 3)
- Sample Talking Points (Attachment 4)
- Sample Notification Letter to Patients (Attachment 5)
- Sample Media Notification Statement/Release (Attachment 6)
- Sample Notification Letter to Secretary of Health & Human Services (Attachment 7)
- Sample Breach Notification Log (Attachment 8)

Written by: Mary Boltik, RHIA

Reviewed by the BHD HIPAA Implementation Team:

Brian Lecus  
Lynn Gram  
Susan Moeser  
Chuck Sigurdson  
Thomas Harding M.D.

Approved by:

<sup>18</sup> HHS issued guidance on protecting personally identifiable healthcare information; document was the work of a joint effort by HHS, its Office of the National Coordinator for Health Information Technology and Office for Civil Rights, and the CMS (Issued 4/17/09).

<sup>19</sup> 45 CFR § 164.103.

## Attachment 1

### Breach Penalties

Penalties for Breach: Penalties for violations of HIPAA have been established under HITECH as indicated below. The penalties do not apply if BHD did not know (or by exercising reasonable diligence would not have known) of the violation or if the failure to comply was due to a reasonable cause and was corrected within thirty days. Penalties will be based on BHD's culpability for the HIPAA violation. The Secretary of HHS will base its penalty determination on the nature and extent of both the violation and the harm caused by the violation. The Secretary still will have the discretion to impose corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation.

The maximum penalty is \$50,000 per violation, with a cap of \$1,500,000 for all violations of an identical requirement or prohibition during a calendar year.

The minimum civil monetary penalties are tiered based upon the entity's perceived culpability for the HIPAA violation, as follows:

**Tier A** – *If the offender did not know*

- \$100 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed \$25,000.

**Tier B** – *Violation due to reasonable cause, not willful neglect*

- \$1,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed \$100,000.

**Tier C** – *Violation due to willful neglect, but was corrected.*

- \$10,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed \$250,000.

**Tier D** – *Violation due to willful neglect, but was NOT corrected.*

## Attachment 2

### Examples of Breaches of Unsecured Protected Health Information

- Workforce members access the electronic health records of a well known public person who is treated within the facility.
- Stolen lost laptop containing unsecured protected health information.
- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).
- Posting of patient's HIV+ health status on Facebook by a laboratory tech who carried out the diagnostic study.
- Misdirected e-mail listing drug seeking patients to an external group.
- Lost flashdrive, containing database of patients participating in a clinical study.
- Staff person accessing the health record of divorced spouse for information to be used in a custody hearing.
- Workforce members accessing electronic health records for information on friends or family members out of curiosity/without a business-related purpose.
- Staff takes a cell phone picture of patient following a Motor Vehicle Accident and transmits photo to friends.
- Misfiled patient information in another patient's medical records, which is brought to the organization's attention by the patient.
- Medical record copies in response to a payer's request are lost in mailing process and never received.
- Misdirected fax of patient records to a local grocery store instead of the requesting provider's fax.
- Briefcase containing patient medical record documents stolen from car.
- PDA with patient-identifying information lost.
- Intentional and non-work related access by staff member of neighbor's information.
- Medical record documents left in public access cafeteria.
- Billing clerk acknowledges diagnosis codes to a 19-year-old patient's mother without consent.

<b>Risk Assessment Analysis Tool</b>
--------------------------------------

Note: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule

Q#	Question	Yes - Next Steps	No - Next Steps
<b>Unsecured PHI</b>			
1	Was the impermissible use/disclosure unsecured PHI (e.g., not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary)?	Continue to next question	Notifications not required. Document decision.
<b>Minimum Necessary</b>			
2	Was more than the minimum necessary for the purpose accessed, used or disclosed?	Continue to next question	May determine low risk and not provide notifications. Document decision.
<b>Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?</b>			
3	Was it received and/or used by another entity governed by the HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 & FISA of 2002?	May determine low risk and not provide notifications. Document decision.	Continue to next question
4	Were immediate steps taken to mitigate an impermissible use/disclosure (ex. Obtain the recipients' assurances the information will not be further used/disclosed or will be destroyed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
5	Was the PHI returned prior to being accessed for an improper purpose (e.g., A laptop is lost/stolen, then recovered & forensic analysis shows the PHI was not accessed, altered, transferred or otherwise compromised)?	May determine low risk and not provide notifications. Document decision. Note: don't delay notification based on a hope it will be recovered.	Continue to next question
<b>What type and amount of PHI was involved in the impermissible use or disclosure?</b>			
6	Does it pose a significant risk of financial, reputation, or other harm?	Higher risk - should report	May determine low risk and not provide notifications. Document decision.
7	Did the improper use/disclosure only include the name and the fact services were received?	May determine low risk and not provide notifications. Document decision.	Continue to next question
8	Did the improper use/disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), or the information increases the risk of ID Theft (such as SS#, account#, mother's maiden name)?	High risk - should provide notifications	Continue to next question

10/23/2009

Question	Yes - Next Steps	No - Next Steps	Question
9	Did the improper use/disclosure <i>not</i> include the 16 limited data set identifiers in 164.514(e)(2) <i>nor</i> the zip codes or dates of birth? Note: take into consideration the risk of re-identification (the higher the risk, the more likely notifications should be made).	High risk - should provide notifications	May determine low risk and not provide notifications. Document decision.
10	Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals (ex. Limited data set included zip codes that based on population features doesn't create a significant risk an individual can be identified)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
<b>Specific Breach Definition Exclusions</b>			
11	Was it an unintentional access/use/disclosure by a workforce member acting under BHD's authority, made in good faith, within his/her scope of authority (workforce member was acting on BHD's behalf at the time), and didn't result in further use/disclosure (ex. billing employee receives an e-mail containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected e-mail & deletes it)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
12	Was access unrelated to the workforce member's duties (ex. did a receptionist look through a patient's records to learn of their treatment)?	High risk - should provide notifications	Continue to next question
13	Was it an inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same BHD, or its OHCA, <i>and</i> the information was not further used or disclosed (ex. A workforce member who has the authority to use/disclose PHI in that BHD/OHCA discloses PHI to another individual in that same BHD/OHCA and the PHI is not further used/disclosed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
14	Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (Ex. Bills were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable)?	May determine low risk and not provide notifications. Document decision.	Continue to next question. Note: if the bills were not returned as undeliverable, these should be treated as breaches.
15	Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (ex. A nurse mistakenly hands a patient discharge papers belonging to a different patient, but quickly realized the mistake and recovers the PHI from the patient, and the nurse reasonable concludes the patient could not have read or otherwise retained the information)?	May determine low risk and not provide notifications. Document decision.	Document findings.
<b>Burden of Proof:</b> Required to document whether the impermissible use or disclosure compromises the security or privacy of the PHI (significant risk of financial, reputational, or other harm to the individual).			

10/23/2

**Sample Talking Points (Based on an Example) – Document to be Reviewed and Customized Prior to Use**

**Talking Points to Respond to Inquiries About Breach of Unsecured Patient Protected Health Information**

***What Happened***

Describe Incident Objectively (see sample below).

- *An employee of the BHD has been arrested for using the personal health information of XX patients to obtain loans and credit cards.*
- *The employee has been charged with identity theft, bank fraud, and credit card fraud.*
- *The employee also illegally obtained \$XXXXX in reimbursement for fraudulent health claims he/she submitted.*
- *The employee allegedly also sold the personal information of our patients to her brother. He also has allegedly obtained credit cards using the patients' identities.*
- *[Insert Law Enforcement Agency Name] is investigating in order to identify the patients affected by the identity theft.*
- *The employee worked as a supervisor in our claims administration area.*
- *The employee has been suspended without pay. Her access to BHD facilities and any BHD computer systems has been terminated.*
- *As a supervisor, the employee had access to personal information of BHD patients.*
- *Her access to patient information was based on her ability to do the job she was assigned.*
- *The employee has been with the BHD for XX years.*
- *The employee underwent a full background check, including criminal check, upon her hire in 20XX.*
- *There have been no other charges against this employee in her time at BHD.*
- *This is the first and only time this type of situation has happened at BHD.*
- *BHD has contacted the affected patients and has provided credit monitoring services and a contact for additional guidance.*



### ***What Are We Doing Now***

#### Customize as Applicable

- We are notifying each individual patient that has been affected by the incident and offering resources to answer any questions or concerns that he or she may have about the current situation.
- *We are contacting the Secretary of the Department of Health & Human Services to notify her of the breach.*
- *We are working with our Compliance Department, IT Department, Legal Department, and Human Resources, to review procedures to see if there are additional safeguards we should implement to prevent this type of action in the future.*
- *We are working with the law enforcement officials to provide them with any information to expedite the investigation and prosecution of this matter.*

### ***What We Will Do for Our Patients***

- *We will continue to make our compliance department available if patients have any questions or concerns regarding their credit.*
- *We have established a special toll-free number for BHD patients to call who have questions regarding their personal information.*
- *We will also encourage patients to contact any of the three credit reporting agencies and establish a fraud alert.*

**Sample Notification Letter to Patients – Document to be Reviewed and Customized Prior to Use**

[Date]

[Name here]  
[Address 1 Here]  
[Address 2 Here]  
[City, State Zip Code]

Dear [Name of BHD Patient or Patient Name]:

I am writing to you with important information about a recent breach of your personal information from the Milwaukee County Behavioral Health Division. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include 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 BHD 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.

***Other Optional Considerations:***

To help ensure that this information is not used inappropriately, BHD will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [Need to document the process for how this would work].

We also advise you to immediately take the following steps:

- Call the toll-free numbers of anyone of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms

your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

- **Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241.
  - **Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013.
  - **TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.
- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
  - Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. BHD apologizes for the stress and worry this situation has caused you and is doing everything it can to rectify the situation.

We have established a toll-free number to call us with questions and concerns about the loss of your personal information. You may call [Insert Toll Free Number] during normal business hours with any questions you have.

We have also established a section on our Web site with updated information and links to Web sites that offer information on what to do if your personal information has been compromised.

**[Insert Closing Paragraph Based on Situation]**

Sincerely,

[Insert Applicable Name/Contact Information]

**Sample Media Notification Statement/Release – Document to be Reviewed and Customized Prior to Use**

[Insert Date]

**Contact:** [Insert Contact Information Including Phone Number/E-Mail Address]

**IMMEDIATE RELEASE**

**MCBHD NOTIFIES PATIENTS OF BREACH OF UNSECURED PERSONAL INFORMATION**

The Milwaukee County Behavioral Health Division (BHD) notified [Insert Number] patients of a breach of unsecured personal patient protected health information after discovering the following event:

Describe event and include the following information as communicated to the victims:

- 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 BHD 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, and/or postal address.

In conjunction with local law enforcement and security experts, BHD is working to notify impacted patients to mitigate the damages of the breach. BHD has in place safeguards to ensure the privacy and security of all patient health information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risk.

In a notification to patients, BHD has offered their resources as well as .... [Insert as Applicable]. BHD also has encouraged its patients to contact their financial institutions to prevent unauthorized access to personal accounts.

BHD has trained staff available for patients to call with any questions related to the data breach. Patients may call [Insert Phone Number Here] from [Insert Hours] with any questions. In addition, patients may visit BHD's Web site at [Insert Web Address] for further information.

BHD understands the importance of safeguarding our patients' personal information and takes that responsibility very seriously," said [Insert Name ] Administrator. "We will do all we can to work with our patients whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to prevent future such occurrences. We appreciate our patients support during this time.

Please direct all questions to [Enter Contact Information].

**Sample Media Notification Statement/Release – Document to be Reviewed and Customized Prior to Use**

[Insert Date]

**Contact:** [Insert Contact Information Including Phone Number/E-Mail Address]

**IMMEDIATE RELEASE**

**MCBHD NOTIFIES PATIENTS OF BREACH OF UNSECURED PERSONAL INFORMATION**

The Milwaukee County Behavioral Health Division (BHD) notified [Insert Number] patients of a breach of unsecured personal patient protected health information after discovering the following event:

Describe event and include the following information as communicated to the victims:

- 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 BHD 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, and/or postal address.

In conjunction with local law enforcement and security experts, BHD is working to notify impacted patients to mitigate the damages of the breach. BHD has in place safeguards to ensure the privacy and security of all patient health information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risk.

In a notification to patients, BHD has offered their resources as well as .... [Insert as Applicable]. BHD also has encouraged its patients to contact their financial institutions to prevent unauthorized access to personal accounts.

BHD has trained staff available for patients to call with any questions related to the data breach. Patients may call [Insert Phone Number Here] from [Insert Hours] with any questions. In addition, patients may visit BHD's Web site at [Insert Web Address] for further information.

BHD understands the importance of safeguarding our patients' personal information and takes that responsibility very seriously," said [Insert Name ] Administrator. "We will do all we can to work with our patients whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to prevent future such occurrences. We appreciate our patients support during this time.

Please direct all questions to [Enter Contact Information].

**Sample Notification Letter to Secretary of Health & Human Services – Document to be Reviewed and Customized Prior to Use**

[Date]

Secretary of Health & Human Services  
The U.S. Department of Health and Human Services  
200 Independence Avenue, S.W.  
Washington, D.C. 20201  
Telephone: 202-619-0257  
Toll Free: 1-877-696-6775

Dear Secretary:

In compliance with the American Recovery and Reinvestment Act of 2009 (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), we are notifying you of a recent breach of unsecured protected health information (PHI). The breach involved [Insert Number] patients. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information as communicated to the victims:

- 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 BHD 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, and/or postal address.
- F.

On behalf BHD I am communicating this information to you in compliance with ARRA/HITECH.

If you have any questions or require further information, please contact me at [Insert Contact Information].

Sincerely,



**Sample Breach Notification Log**

BHD shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. A record of the complete investigation of the potential breach as well as the risk assessment carried out to determine notification requirements should be created. The risk assessment and the record/incident report should be cross-referenced so that should the Secretary of HHS require more information, it is easy to locate and provide.

Note: Reconfigure Width of Data Fields for Landscape Document or Spreadsheet

Incident #	Date of Discovery	Date of Breach	Location	Brief Description of Breach*	Number Patients Involved	Notification Dates			Actions Taken Resolution Steps
						Patients	Media	HHS	

- A description of what happened, including 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, etc.).

POLICY AND PROCEDURE	DATE ISSUED 10/93	SECTION-CENTRAL ADMINISTRATION	P&P NO. ADM-4	PAGE 1 of 2
----------------------	----------------------	-----------------------------------	------------------	----------------

MILWAUKEE COUNTY  
BEHAVIORAL HEALTH  
DIVISION

DATE REVISED:  
10/95, 10/08

SUBJECT:  
CONFIDENTIALITY PROCEDURE -  
CLIENT INFORMATION

**POLICY:**

All Milwaukee County Behavioral Health Division (BHD) treatment information/records must remain confidential whether learned of verbally, stored in hard copy, or on computer, and are privileged according to Wisconsin Mental Health Act Chapter 51, Federal Regulations 42 CFR Part 2, and Health Insurance Portability and Accountability Act (HIPAA).

All BHD employees/contract agency employees/students and all others who have access to information in order to perform their job description shall sign a confidentiality statement at the time of their BHD orientation which will signify their willingness to abide by BHD policy and procedures, state statutes, and federal regulations. The statement will be filed in the employee's personnel file maintained in the BHD Human Resources Department, or in the case of a contract agency employee, at the place of employment.

**PURPOSE:**

To comply with State Statutes and Federal Regulations and to assure Behavioral Health Division patients that their confidentiality will be protected.

**PROCEDURE:**

**RESPONSIBILITY**

**ACTION**

ALL BHD EMPLOYEES

1. Any patient identity and/or patient treatment information whether learned of verbally, stored on hard copy, or on computer, shall be considered confidential and may only be disclosed to authorized persons with the express, written, informed consent of the patient or through statutory regulation as specified in Wisconsin Mental Health Act Chapter 51, Federal Regulations 42 CFR Part 2, HFS 92, or HIPAA.
2. Any patient identity and/or patient treatment information may only be shared with fellow employees who are providing direct services to the patient and/or as necessary in the performance of their jobs. Supervisory and administrative personnel may have access to this information as needed in the performance of their position description.
3. Computerized files are to be treated in the same confidential manner as the written medical record. Computerized information shall be accessed only as is necessary to fulfill job requirements. The information contained in the computer should be treated impersonally and not discussed with anyone except as it pertains to job responsibilities. It is imperative that access ID's are kept confidential and computers are signed off or locked every time an employee is away from their desk.
4. Any document that identifies a patient or includes patient information (whether it be the actual hard copy medical record or electronic media) is not to be removed from the Behavioral Health Division and/or its satellite offices (including contracted services), except as is necessary to perform job responsibilities and as allowed in the State Statutes, Federal Regulations, or BHD policy. Employees who remove information under this provision are to have supervisory approval and are responsible for protecting the information appropriately.

POLICY AND PROCEDURE	DATE ISSUED 10/93	SECTION-CENTRAL ADMINISTRATION	P&P NO. ADM-4	PAGE 2 of 2
MILWAUKEE COUNTY BEHAVIORAL HEALTH DIVISION	DATE REVISED: 10/95, 10/08	SUBJECT: CONFIDENTIALITY PROCEDURE - CLIENT INFORMATION		

RESPONSIBILITY

BHD DEPARTMENT HEAD  
AND/OR DESIGNEE

ACTION

- All staff working at BHD will be required to sign a General Confidentiality Statement. Staff who have access to confidential information or the computer system will need to sign an additional statement, of which a copy *must* be forwarded to IMSD in order to gain computer access. Both statements will be maintained in their personnel folder.
- Whenever an individual leaves employment, IMSD shall be notified immediately to delete the employee's passwords.

Revised by:           The BHD HIPAA Implementation team  
                           Chuck Sigurdson  
                           Brian Lecus  
                           Lynn Gram  
                           Mary Boltik  
                           Patricia Walslager

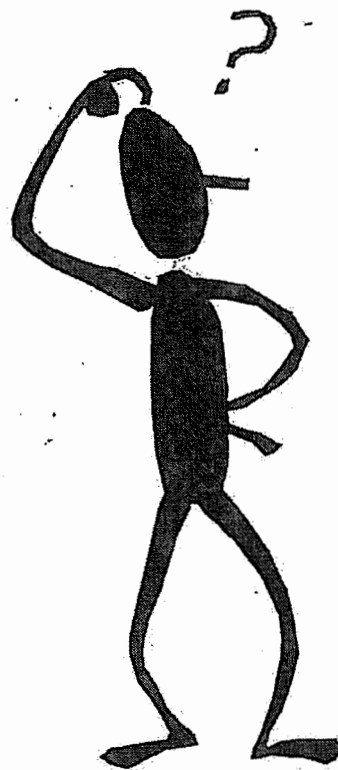
Reviewed and approved by Mary Boltik RHIA, Dir- Medical Records



## ***What is HIPAA?***

---

**HIPAA** is the  
**H**Health  
**I**nsurance  
**P**ortability and  
**A**ccountability  
**A**ct of 1996



## ***What does HIPAA protect?***

---

HIPAA requires us to respect and protect the privacy of what is called  
**“protected health information”(PHI)**

PHI is health information that we maintain or share that could be used to identify an individual, including:

- name
- address
- date of birth
- phone number
- Social Security Number
- medical record number
- account number for billing
- e-mail address
- photographs of the individual

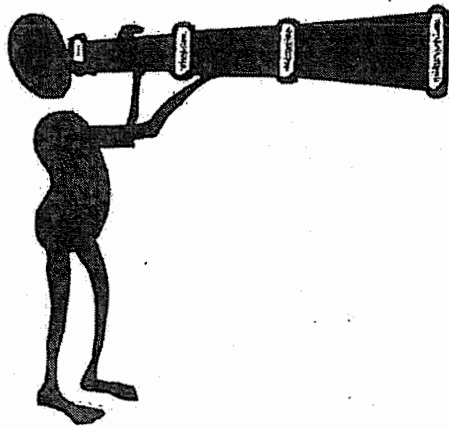
and any other information that specifically identifies a person who is receiving treatment or service.



## Where is PHI found?

---

Protected Health Information is contained in the medical record, but it is also found in many other places within the organization:



- in conversations:  
our verbal discussions with each other
- computer files
- papers files
- billing records
- lists and rosters
- messages to each other

Look around and you'll see that information about the people we serve is all around us in our organization!



## ***Who gets to see Protected Health Information?***

---

HIPAA says that employees are only allowed to see (or hear) the “**minimum necessary**” information to do their job.

- for example, a physician would need to see the entire record to provide treatment
- however, a dietary worker would only need to know the individual’s name and unit to label a nourishment for an individual.
- a manager would need to see the entire record to supervise their employees
- however, a housekeeper would only need to know the room number to clean the room for a specific patient or resident.



## ***Won't HIPAA privacy rules keep us from doing our jobs?***

---

The **welfare of individuals**, specifically in crisis situations, takes priority over privacy concerns.

HIPAA **does** allow us to use protected health information within the organization for the purpose of doing our work.

HIPAA identifies three specific purposes for which we may use protected health information:

**T**reatment

**P**ayment for health care services

**O**peration of the health care system

These three types of information are referred to by their initials as **TPO**

However, Wisconsin state law sets a **higher** standard that still requires us to obtain consent for billing, and for some treatment uses.





## ***What is disclosure?***

---

**Disclosure** means any way in which we release, share, or allow others to have access to health information - verbally, electronically or in writing.

We may disclose information officially with the individual's permission, such as when a social worker sends records to a clinic or program who will provide follow-up care, and the individual has signed an authorization form.

We also sometimes disclose information **incidentally**, such as when others overhear us speak - in spite of our safeguards to protect privacy.



## ***What if information DOES get out?***

---

### **There are two ways PHI might get out:**

Information might get out in spite of all our careful efforts to protect privacy. HIPAA calls this **“incidental disclosure”**.

An example might be when another individual hears us talking with a patient about their care

Information might also get out by accident when we are careless and do not follow HIPAA privacy procedures. HIPAA call this **“accidental disclosure”**.

When this occurs, we need to report these accidental disclosures to the supervisor and to the Privacy Officer who will log the disclosure

HIPAA requires us to always use **reasonable safeguards** to protect against incidental disclosure. Examples might be:

- ask the patient to move with you to a private place to talk, or
- speak softly so others nearby cannot hear



## NEW IMPORTANT HIPAA POLICY

A new policy, "**Breach Notification-Protected Health Information Policy**" was recently enacted as a result of a new law known as the Health Information Technology for Economic and Clinical Health Act (HITECH). You can refer to the computerized version at anytime via one of these two methods.

In the Inpatient areas - click on the "**Shortcut to BHD Procedures**" icon located on the PC desktop then access the Admin &or Division Wide folder and then the Hospital Policies folder. Staff with BHD Network access may go directly to the indicated section(s)\* of **H:\BHD Procedures / Health Information Management**.

First implemented on September 23, 2009 with full compliance needed by February 22, 2010.

### **Key Points are:**

If BHD or any staff member within BHD accidentally disclose patient information, it needs to be reported on a BHD Incident Form, inform the BHD HIPAA Privacy Officer (Mary Boltik, at x6953).

Once reported, an investigation will be conducted, including a risk assessment to determine the potential harm to the patient from the disclosure. The investigation will determine if the patient, Director of Health and Human Services, and/or the media need to be notified.

The law also created monetary penalties to the organization and monetary penalties to the individual staff member that releases the information. HITECH penalties range from \$100 per occurrence up to a maximum of \$50,000 per occurrence. An individual may be subject to internal discipline within BHD **AND** civil action for the disclosure which could include fines up to \$25,000 and up to 9 months in jail.

It is VERY important to keep patient information secure at all times. Please refer to the policy attachment 2 for examples of breaches.