DMH Compliance Alert

Privacy and Security is Everyone's Business

January 2006

HIPAA Security and the DMH Information Security Officer

As you may know, the HIPAA Security Rule went into effect on April 20, 2005. DMH has named Jane Trott as the DMH Information Security Officer.

Jane comes to Central Office from the North East Area IT Department. Jane can be reached at 617-626-8186 or on the DMH Information Security Officer phone line at 617-626-8187. She can also be sent e-mail at Jane.Trott@dmh.state.ma.us.

DMH also has established a HIPAA Security workgroup. This workgroup has been working for the past year on creating a DMH Security Handbook that will set forth the statewide procedures that will ensure DMH compliant with the HIPAA Security Rule standards.

The HIPAA Security Rule requires that DMH ensure the security, availability and reliability of Electronic Protected Health Information (EPHI). In many circumstances there is overlap between the HIPAA Security Rule and the HIPAA Privacy Rule. An example of this overlap is that the authority for EPHI to be disclosed outside of the DMH workforce is a privacy issue (i.e. is there an authorization, court order, etc.) while the mechanics of how it gets released is a security issue (i.e. use of the Secure File Email Delivery System).

Once the DMH Security Handbook is finalized all DMH workforce members will be trained as appropriate to their job functions. The DMH Security Handbook will be available on the DMH Intranet page for DMH workforce members' use.

INSIDE THIS ISSUE

- HIPAA Security Rule
- Response to Request to Access or Inspect PHI
- Disclosing PHI
- Accessing PHI
- Privacy and Compliance Link
- Privacy Training Update
- Audit Trails
- Statewide Record Retention Schedule

Response to a Request to Inspect Protected Health Information (PHI)

Staff are reminded of the following when responding to an individual, or his or her Personal Representative (PR), requesting to inspect or receive a copy of his or her PHI:

- Except in very limited circumstances an individual, or his/her PR, has the right to inspect or request a copy of the individual's PHI that is maintained in a DMH Designated Record Set.
- An individual, or his/her PR, can only be denied access to the individual's PHI for very specific reasons such as if a licensed health care professional determines that access is reasonably likely to endanger the life or physical safety of the individual or another person.
- A request to inspect or copy PHI must be documented in writing. *The DMH Request to Inspect or Receive a Copy of PHI* form can be used but is not required.
- The response to a request must be made within 30 days.
- Among other things, a Safety Determination must be made using Page 2 of *the DMH Request to Inspect or Receive a Copy of PHI* prior to releasing the requested PHI.
- A denial (in whole or in part) must be done in writing using the *DMH Access Request Denial Letter*.
- A complete list of the only circumstances when access can be denied can be found in the DMH Privacy Handbook Chapter 11 Section II, B.
- If you receive a request to inspect PHI from an individual or his or her PR please forward it the appropriate DMH workforce member as listed in Chapter 11 of the DMH Privacy Handbook.

Chapter 11 of the DMH Privacy Handbook provides more specific details on this topic. All referenced letters and forms can be found on the DMH Privacy Page on the DMH Intranet.

Below is a direct link to Chapter 11:
http://www.dmh.state.ma.us/Intranet/CommonFiles/HIPAA/HandbookPDF/Ch_11%20Access.pdf

Please contact your Area Privacy Coordinator or the DMH Privacy Officer if you have questions.

Disclosing PHI

DMH workforce members are never to disclose information about an individual who has applied for, is receiving or has previously received services from DMH, unless that disclosure is permitted according to the DMH Privacy Handbook.

If a high profile individual is sent from the court system to a DMH facility, information can not be released about the individual unless permitted according to the DMH Privacy Handbook. Even if the news media is reporting that the individual is at a DMH facility, generally DMH workforce members are not allowed to either confirm or deny that the individual is being served by DMH without proper Authorization from the individual, or his/her PR.

Accessing PHI

DMH Workforce members are reminded that they may only access that PHI which is necessary to perform their job. In recent months a number of workforce members were notified of the rollout of the INFORM system. This information system is designed to assist certain DMH workforce members to access reports and data from the MHIS system in ways that are not currently available via MHIS. Access to INFORM will be limited to those workforce members for whom access is necessary to perform their job functions,

Privacy and Compliance Link

A new Privacy and Compliance link has been added to the DMH Intranet web page. This link can be found on the top right corner of the DMH Home page under the Commissioner's Office heading.

The link will direct users to the DMH Privacy and Compliance page. This page lists the DMH Area Privacy Coordinators. In the future this page will also list the Area Security Coordinators.

Also on the DMH Privacy and Compliance page is the "Get HIPAA" icon which brings staff to the DMH Privacy Page. On the DMH Privacy page is the DMH Privacy Handbook, DMH Privacy forms and letters, DMH Compliance Alerts and other important Privacy related documents.

Below is a direct link to the DMH Privacy and Compliance page:
http://www.dmh.state.ma.us/Intranet/StaffList/PrivacyandCompliance.asp?LID=74&H1=Privacy+and+Compliance

Privacy Training Update

Most DMH workforce members have completed the DMH-specific Privacy training. Workforce members were trained on either the Basic, Intermediate or Advanced level depending on their job functions. If you have not yet completed your training please contact your Area Staff Development Office to schedule a session.

Audit Trails

An individual, or his/her PR, has the right to an audit trail of certain types of disclosures of the individual's PHI that are made by DMH. A disclosure is the release, transfer, provision of access to, or divulging in any other manner of PHI outside of the DMH Workforce. The types of disclosures subject to this rule are found in Chapter 12, Section II.A, of the DMH Privacy Handbook.

A DMH workforce member making a disclosure that is subject to the audit trail rule must ensure that the disclosure is logged appropriately.

How this requirement is put into practice may be specific to your facility. Please check with your Area Privacy Coordinator and/or facility Medical Records Director as to logging procedures applicable to your DMH site.

Remember disclosures can only be made if permitted by the DMH Privacy Handbook. Logging a disclosure on an Audit Trail does not replace the need for proper authorization (See Chapter 6 of the DMH Privacy Handbook).

Below is a direct link to Chapter 12 of the DMH Privacy Handbook:
http://www.dmh.state.ma.us/Intranet/CommonFiles/HIPAA/HandbookPDF/Ch_12%20RightToAnAuditTrail.pdf

Below is a direct link to Chapter 6 of the DMH Privacy Handbook:
http://www.dmh.state.ma.us/Intranet/CommonFiles/HIPAA/HandbookPDF/Ch_06%20Uses&Disclosures.pdf

Statewide Record Retention Schedule

As the new year begins staff are reminded that as a state agency, all documents created or received by DMH workforce members, in any media, are subject to the Statewide Record Retention Schedule. Staff must consult the Schedule before destroying any documents.

The current Schedule can be found on the Secretary of State's Public Records Division web page or through the link below:
http://www.sec.state.ma.us/arc/arcrmu/rmurds/05-05ApprovedCopy.doc

At the end of the Schedule there is an index which will assist you in navigating the Schedule.

DMH is in the process of requesting some language changes to the next version of the Schedule. However, these will not involve changes in length of retention. DMH workforce members will be notified when the next Schedule is approved and published.

Please feel free to contact Grace Beason with any questions regarding use of this Schedule.

Questions about this bulletin may be directed to:
Grace Beason, LICSW, Director of Privacy & Compliance
617-626-8163
Jane Trott, DMH Information Security Officer
617-626-8186
Department of Mental Health
25 Staniford Street
Boston, MA 02114