

DEPARTMENT OF MENTAL HEALTH AND DEVELOPMENTAL DISABILITIES

POLICIES AND PROCEDURES

Subject:
ADMINISTRATION OF HIPAA

Effective Date:
12/15/03

Policy Number:
HIPAA 03-1

Review Date:
6/8/06
Revision Date:
11/21/06

Entity Responsible:
Office of Legal
Counsel

(All legal citations will be moved to the “Authority” section of this policy.)

1. Purpose:

To provide a process to designate personnel to develop, implement and administer the Department of Mental Health and Developmental Disabilities’ (DMHDD) policies and procedures that comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, federal laws, and the Tennessee Code Annotated. **45 C.F.R. § 164.530; 42 U.S.C.A. § 1320d; Tenn. Code Ann. §§ 33-3-103, et seq.**

2. Policy:

2.1 The DMHDD Commissioner shall designate a HIPAA Compliance Officer (DMHDD Privacy Officer) who is responsible for administering, developing, and implementing the policies and procedures of the DMHDD pursuant to HIPAA rules and regulations, as well as federal and state laws. This designation must be documented and maintained for six (6) years. The Privacy Officer shall be a licensed attorney serving in the Office of Legal Counsel, DMHDD Central Office, and shall be able to understand, interpret, explain, and ensure departmental compliance, with federal and state laws and regulations concerning safeguarding privacy and security. **45 C.F.R. § 164.530(a) through (i); 65 Fed. Reg. 82561 (Dec. 28, 2000); Employer’s Guide to HIPAA Privacy Requirements, §§ 510 through 513, pp. 51 through 57 (Nov. 2004); Tenn. Code Ann. § 33-1-303.**

2.2 The DMHDD shall designate a contact person who is responsible to document, process and dispose of HIPAA complaints, who is able to provide information about matters concerning adequate notice of the uses and disclosures of protected health information (PHI). This person shall work to ensure that any person wanting to file a complaint is not intimidated, threatened, coerced, discriminated against or retaliated against by any member of the DMHDD workforce. The DMHDD Privacy Officer shall serve as the DMHDD contact person. **45 C.F.R. § 164.530(a); 65 Fed. Reg. 82561 (Dec. 28, 2000); Tenn. Code Ann. § 33-1-303.**

3.1.1 2.3 Each Regional Mental Health Institute (RMHI) Chief Officer shall designate a HIPAA Privacy Officer (RMHI Privacy Officer) who provides

information about the use, disclosure, and safeguarding of PHI; and implements the policies and procedures of the RMHI under HIPAA privacy rules and regulations. This designation must be documented and maintained for six (6) years. Each RMHI must have a contact person to document and process complaints. The RMHI Privacy Officer of each facility shall serve as the contact person for the RMHI. **45 C.F.R. § 164.530(a) through (i); 65 Fed. Reg. 82561 (Dec. 28, 2000); Tenn. Code Ann. § 33-1-303.**

- 2.4 The Commissioner of the DMHDD shall designate a HIPAA Security Officer (DMHDD Security Officer) who is responsible for the implementation of the security policies and procedures of the DMHDD under HIPAA security rules and regulations, to prevent, detect, contain, and correct HIPAA security violations. This designation must be documented and maintained for six (6) years. The DMHDD Security Officer shall have an information systems background, work in the Information Systems section of the DMHDD Central Office, and shall be familiar with federal and state laws and regulations concerning information security. **45 C.F.R. § 164.308(a); Tenn. Code Ann. § 33-1-303.**
- 2.5 Each RMHI Chief Officer shall designate a HIPAA Security Officer (RMHI Security Officer) who implements the policies and procedures of the RMHI under HIPAA security rules and regulations, to prevent, detect, contain, and correct HIPAA security violations. This designation must be documented and maintained for six (6) years. **45 C.F.R. § 164.308(a); Tenn. Code Ann. § 33-1-303.**
- 2.6 The DMHDD shall have a HIPAA Officers Committee comprised of the DMHDD Privacy Officer, who will serve as Chair; the DMHDD Security Officer, who will serve as Vice Chair, and the RMHI Privacy and Security Officers, who will serve as members. **Tenn. Code Ann. § 33-1-303.**
- 2.7 The DMHDD shall have a five-person HIPAA Advisory Committee (HAC) to assist the DMHDD Privacy and Security Officers in implementing the objectives of HIPAA, by offering advise and counsel, and by performing those duties that may from time to time be assigned them by the HAC. The HAC shall consist of the DMHDD Privacy and Security Officers, a representative from Administrative Services, a representative from the Office of Hospital Services and a representative from one of the RMHIs. **Tenn. Code Ann. § 33-1-303.**

3. Procedure/Responsibility:

- 3.1 Duties of the DMHDD Privacy Officer:
 - 3.1.1 Develop HIPAA programs, publish and distribute the updated HIPAA privacy notice; maintain HIPAA policies and procedures in written or electronic form. **45 C.F.R. § 164.530(a), (i), and (j).**

- 3.1.2 Oversee maintenance of the DMHDD HIPAA Privacy Intranet site. Document that all HIPAA privacy policies are accessible to all Privacy and Security Officers and DMHDD employees, to assist in their compliance, via the Intranet site, and made available to consumers via Internet access through the DMHDD web site. **45 C.F.R. § 164.530(a) and (i).**
- 3.1.3 Monitor compliance with HIPAA rules, regulations, policies and procedures; require appropriate sanctions against workforce members who fail to comply with privacy policies and procedures; change policies and procedures as needed. **45 C.F.R. § 164.530(a) through (i).**
- 3.1.4 Serve as the designated decision maker for legal issues concerning HIPAA regulations, policies and procedures, and provide assistance and guidance to DMHDD Directors, RMHI Attorneys, and RMHI HIPAA Officers, involving the interpretation and application of the HIPAA rules and regulations, as well as applicable federal and state laws. **45 C.F.R. § 164.530(a) through (i); Tenn. Code Ann. § 33-1-303.**
- 3.1.5 Develop procedures to ensure that each new member of the DMHDD workforce is trained on HIPAA privacy rules, policies and procedures, and document this training by requiring each trainee to sign a statement certifying that s/he received privacy training. **45 C.F.R. § 164.530(b); 45 C.F.R. § 164.530(e)(1).**
- 3.1.6 Ensure appropriate administrative, technical, and physical safeguards are in place to protect the privacy of PHI, and to reasonably safeguard PHI from intentional or unintentional use or disclosure. **45 C.F.R. § 164.530(c).**
- 3.1.7 Provide a process for individuals to make complaints, to have the complaints documented, and to ensure investigation and disposition of complaints; ensure that any person seeking to file a complaint is not intimidated, coerced, threatened, or subjected to other retaliatory action. **45 C.F.R. § 164.530(d); 45 C.F.R. § 164.530(g)(1).**
- 3.1.8 Maintain working relationships with other state agencies and covered entities in the private sector concerning HIPAA issues. **Tenn. Code Ann. § 33-1-303.**
- 3.1.9 To the extent required by law, maintain contact with the U.S. Department of Health and Human Services, Office of Civil Rights (OCR), and the Centers for Medicare and Medicaid Services (CMS), consistent with HIPAA rules and regulations, understand HIPAA audit requirements and methodologies, and report HIPAA violations as required by law. **45 C.F.R. § 164.530.**

- 3.1.10 Ensure that Business Associate Agreements (BAA) are developed as required by HIPAA rules and regulations for business associates of the DMHDD, and of the RMHIs, as well as prepare BAAs as needed. **45 C.F.R. Parts 160 and 164.**
- 3.1.11 Perform other responsibilities as delineated in the DMHDD HIPAA policies and procedures. **Tenn. Code Ann. § 33-1-303.**
- 3.2 Duties of the RMHI Privacy Officers:
 - 3.2.1 Each RMHI HIPAA Privacy Officer must ensure that all RMHI workforce is trained in HIPAA privacy regulations, as well as DMHDD and RMHI privacy policies. **45 C.F.R. § 164.530(b).**
 - 3.2.2 Ensure appropriate safeguards at the RMHI are in place to protect the privacy of PHI. **45 C.F.R. § 164.530(c).**
 - 3.2.3 When serving as the RMHI contact person, to document and investigate complaints at the RMHI, and work toward their resolution. **45 C.F.R. § 164.530(d).**
 - 3.2.4 Perform other responsibilities as delineated in the DMHDD and RMHI HIPAA policies and procedures. **45 C.F.R. § 164.520; Tenn. Code Ann. § 33-1-303.**
- 3.3 Duties of the DMHDD Central Office HIPAA Security Officer:
 - 3.3.1 Assess and reduce risks and vulnerabilities to the security and confidentiality, integrity, and availability of electronic PHI that the DMHDD creates, receives, maintains, or transmits; and protect against reasonably anticipated threats to security. **45 C.F.R. § 164.306(a).**
 - 3.3.2 Periodically review records of information system activity, such as audit logs, access reports, and security incident tracking reports. **45 C.F.R. § 308(a)(ii)(D).**
 - 3.3.3 Develop procedures to ensure that each new member of the DMHDD workforce is trained on HIPAA security rules, policies and procedures, and document this training by requiring each trainee to sign a statement certifying that s/he received security training. Implement procedures to guard against, report and detect malicious software. **45 C.F.R. § 164.530(b); 45 C.F.R. § 164.530(e)(1). 45 C.F.R. § 164.308(a)(5).**

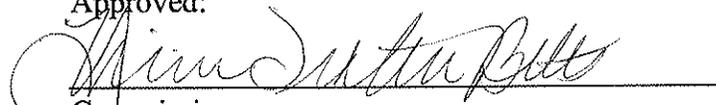
- 3.3.4 Create log-in procedures for computer workstation security; to monitor log-in discrepancies, to safeguard passwords; respond to and document security incidents. **45 C.F.R. § 164.308(a)(5), and (a)(6).**
 - 3.3.5 Ensure that all workforce members have appropriate access to electronic PHI; prevent those who should not have access from obtaining access; implement procedures for terminating access to PHI stored electronically, when a member of the workforce terminates his or her employment. Create procedures to ensure compliance by the DMHDD workforce, and require appropriate sanctions against workforce members who fail to comply with security policies and procedures. **45 C.F.R. §§ 164.306(a)(4); 45 C.F.R. § 164.308(a)(1)(ii)(C).**
 - 3.3.6 Maintain the DMHDD HIPAA Security Intranet site, and make all DMHDD HIPAA Security Policies available to all RMHI Privacy and Security Officers and the DMHDD workforce, via the DMHDD Intranet site, to assist with compliance. Consumers may have access to those policies via the Internet, only if this can be accomplished without compromising the DMHDD's security. **45 C.F.R. § 164.306 (a)(4).**
 - 3.3.7 Establish a contingency plan for responding to an emergency or other occurrence, including data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, and applications and data criticality analysis data used to assess sensitivity, vulnerability and security of key information assets. **45 C.F.R. § 164.308(a)(7)(ii)(A) through (E).**
 - 3.3.8 Provide assistance and guidance to RMHI Security Officers and department personnel as needed. **45 C.F.R. § 164.308(a)(5); Tenn. Code Ann. § 33-1-303.**
 - 3.3.9 Maintain working relationships with other state agencies and covered entities in the private sector concerning HIPAA security issues. **Tenn. Code Ann. § 33-1-303.**
 - 3.3.10 Perform other responsibilities as delineated in the DMHDD HIPAA policies and procedures. **45 C.F.R. § 164.308; Tenn. Code Ann. § 33-1-303.**
- 3.4 The RMHI HIPAA Security Officer's responsibilities include the following:
- 3.4.1 Each RMHI Security Officer must ensure that RMHI workforce are trained in HIPAA security rules and regulations, as well as DMHDD and RMHI security rules. **45 C.F.R. § 164.308(a)(5)(i); 65 Fed. Reg. 82561 (Dec. 28, 2000).**

- 3.4.2 Ensure that all workforce members have appropriate access to electronic PHI; prevent those who should not have access from obtaining access; end access when a member of the workforce terminates employment. **45 C.F.R. § 164.308(a).**
- 3.4.3 Periodically review records of information system activity, such as audit logs, access reports, and security incident tracking reports. **45 C.F.R. § 164.308(a)(ii)(D).**
- 3.4.4 Perform other responsibilities as delineated in the DMHDD and RMHI HIPAA policies and procedures. **45 C.F.R. § 164.308; Tenn. Code Ann. § 33-1-303.**
- 3.5 The Purpose of the HIPAA Officers Committee includes the following:
 - 3.5.1 Keeping all RMHI Privacy and Security Officers current on HIPAA policy changes and issues by their participation in a quarterly conference call. **Tenn. Code Ann. § 33-1-303.**
 - 3.5.2 Providing a forum for discussion and exchange of HIPAA information among the Central Office and RMHI HIPAA Officers, to advance competence in privacy and security knowledge, and to improve compliance with HIPAA rules and regulations and with federal and state laws. **Tenn. Code Ann. § 33-1-303.**

4. Other Considerations:

Authority:

45 C.F.R. § 164.308(a); 45 C.F.R. § 164.530(a); 45 C.F.R. § 164.530(b); 45 C.F.R. § 164.530(g)(1); 45 C.F.R. § 164.530(i); 65 Fed. Reg. 82561 (Dec. 28, 2000); Employer's Guide to HIPAA Privacy Requirements, §§ 510 through 513, pp. 51 through 57 (Nov. 2004); Tenn. Code Ann. § 33-1-303; 42 U.S.C.A. § 1320d.

Approved:

 Commissioner
 11/21/06
 Date