SOUTH CAROLINA DEPARTMENT OF MENTAL HEALTH
Columbia, South Carolina

OFFICE OF THE STATE DIRECTOR OF MENTAL HEALTH

DIRECTIVE NO. 948-21

(5-100)

TO: All Employees

SUBJECT: Privacy Practices

I. PURPOSE

This Directive describes DMH policy for the use and disclosure of DMH Patient medical and payment Protected Health Information or "PHI" and Patient rights related to access, control, accounting and amending of their PHI. For purposes of this policy, reference to Patient includes Residents in DMH Long Term Care facilities. This Directive incorporates "Notice Of Privacy Practices" ("Notice", form M-010, Appendix #1), as well as other forms and procedures listed in the Appendix. This Directive includes future Notices, forms or procedures added to the Appendix, and adopted in accord with DMH policy and applicable law.

Each DMH employee, volunteer or other person (e.g., contract physician) incorporated in the DMH workforce ("workforce member" or "staff") and officials, must sign acknowledgement of receipt of, and agreement to comply with this Directive "SCDMH Privacy Practices Acknowledgement and Agreement" (form HRS-2, Appendix #2). The signed statement must be kept in the applicable personnel or other official folder. Each DMH component must ensure training of its staff consistent with this Directive and DMH Privacy Practices training. All DMH component policies or agreements must be consistent with this Directive.

II. APPLICABLE LAW

This Directive is to conform with, and is subject to, applicable federal and state law, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Section 44-22-100 of the Code of Laws of South Carolina. In general, DMH is required by law to: follow the Notice requirements; keep Patient information private; give Patients the opportunity to review the Notice and request restrictions on PHI use or disclosure; not use or share PHI without Patient Authorization except as described in the Notice; provide for Patient rights involving control over his or her PHI; and a procedure for Patient complaints about DMH privacy practices.

Identifying information from Substance Use Disorder (SUD) treatment programs (formerly referred to as Alcohol and Drug (A&D) treatment programs), is subject to additional restrictions and protections under federal law 42 CFR Part 2. If in doubt as to whether 42 CRF Part 2 applies to a DMH program, the applicable local director should consult with the DMH

Office of General Counsel. 42 CFR Part 2 applies to any "federally assisted" SUD treatment "Program" and DMH inpatient and outpatient facilities and programs that are "federally assisted". Records from any DMH inpatient or outpatient facility or program that holds itself out as a Substance Use Disorder (SUD) "Program", are protected by Federal Law (42 CFR Part 2). 42 CFR Part 2 defines a SUD "Program" as an entity that "holds itself out" as a SUD program providing alcohol or drug abuse diagnosis, treatment or referral for treatment. If a CMHC Co-occurring Disorder program "holds itself out" as a SUD Program, then it is a "Program" as defined in 42 CFR Part 2 and ALL "Program" records are covered by 42 CFR Part 2. 42 CFR Part 2 is much more restrictive than HIPAA and Does NOT Allow Many Disclosures Permitted By HIPAA/Other Law.

Additional requirements (e.g., for licensing, accreditation, etc.) may also apply to individual DMH components.

III. PROCEDURES

1. Notice

A copy of the current DMH Notice must be posted at each service site where persons seeking DMH services will be able to read it. When DMH changes the Notice, a current copy must be posted in like manner. A copy of the Notice must also be posted on the DMH Internet Web site. Patients must have the opportunity to review the Notice and receive a paper copy at any time. This acknowledgment is to be documented on (revised July 2021) "Consent To Examinations And Treatment" (form C-107, July 2021, Appendix #3) or an applicable intake or admission form, containing the statement (or an attached statement):"I have been provided a copy of the SCDMH Notice of Privacy Practices and an opportunity to review it and ask questions." If not signed, staff must note on the signature line of the statement, why signed acknowledgement was not obtained (e.g., "refused a copy of the Notice", "refused to sign", etc.) Questions concerning the Notice, this Directive, or DMH Privacy Practices should be directed to the local Privacy Officer or the DMH Privacy Officer.

2. DMH Uses and Disclosures of PHI

After providing the Patient with the opportunity to review the Notice, and object and/or request certain restrictions, staff may share PHI as described in the Notice. In an emergency or if the Patient is incapacitated, without giving the Patient the opportunity to review the Notice, object or request limitations, DMH may use and/or share PHI as permitted under the Notice. As soon as reasonable after the emergency or incapacity, the Patient must be given those opportunities. When practical and when it will not compromise Treatment, DMH should accommodate a Patient's request to limit PHI use or disclosure. As described in the Notice, PHI may be disclosed pursuant to a Business Associate Agreement, approved by the DMH Contracts Office and the office of the DMH Privacy Officer. DMH workforce members should limit use or disclosure of PHI to the Minimum Necessary to accomplish the purpose for the use or disclosure as described in the Notice.

For use and disclosure of PHI for Operation purposes, applicable component directors must identify employees who need access to PHI to carry out their DMH duties (see

Notice); and the PHI categories to which access is needed and any limitations to such access. For types of disclosure of, or request for, PHI made on a routine and recurring basis, the component must implement protocols limiting the PHI disclosed or requested to the Minimum Necessary to achieve the purpose of the disclosure or request. Protocols must be reviewed and approved by the local Privacy Officer. For other PHI disclosures or requests (i.e., non-routine, non-recurring), the component must develop protocols to limit the PHI disclosed or requested to the Minimum Necessary and review all such requests for disclosure on a case by case basis to determine that the PHI information sought is limited to the Minimum Necessary to achieve the purpose of the specific disclosure or request.

3. **Other Exceptions, Legal Proceedings, Notice of Privacy Law**
Unless disclosure is otherwise permitted by the Notice, upon receipt of a subpoena or other request for PHI, a statement substantially similar to the "Model Notice Of Privacy Law" (Appendix #4) must be sent to the requester. If required to provide testimony or other information containing PHI in a legal proceeding, staff must follow the procedure described in "Disclosures In Legal Proceedings" (Appendix #5).

4. **Authorizations**
Unless permitted by the Notice, PHI may not be disclosed without a signed "Authorization To Disclose SCDMH Protected Health Information" (form M-450D, Appendix #6), to be kept in the Patient's medical record. Requests pursuant to an Authorization must be acknowledged within 15 days of receipt and completed within thirty days. The Authorization to Disclose Protected Health Information to SCDMH (form M450-E, Appendix #7) may be used to request information from entities outside of SCDMH when authorization is required.

5. **Re-Disclosure Notice**
Disclosure of Alcohol and Drug Abuse Patient Records regulations prohibit re-disclosure of health information. Federal regulations 42 CFR Part 2 require that a notice accompany each disclosure made with a patient's written consent. The notice must state: *"The information has been disclosed to you from records protected by federal confidentiality rules (42 CFR Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2",* "Model Notice Prohibiting Re-Disclosure", Appendix #8).

6. **Patient Privacy Rights**
The Notice describes the following Patient PHI privacy rights: receipt of a copy of the Notice and opportunity to review and ask questions; object and request restrictions on some PHI uses or disclosures; request confidential communication/notification; inspect and obtain copy of PHI; request amendment to PHI; receive an accounting of PHI disclosures; and the right to file a complaint with DMH, HHS and Office of Civil rights about DMH privacy practices. As described in the following Section 7, exercise of Patient privacy rights concerning his or her PHI may require that a Patient complete a written

request and follow the noted procedure. Formal Privacy Practice complaints may involve the Privacy Officer and the Patient Advocate.

7. **Patient Access to His or Her Own PHI, Psychotherapy Notes**
Patient has the right to request access and/or copies of his/her PHI as described in the Notice as long as DMH maintains the PHI, "Request To Inspect And/Or Copy SCDMH Protected Health Information", (form M-451, Appendix #9). The DMH component must act on a Patient's request no later than 30 days of the receipt of the request, but may deny access to some information including Psychotherapy Notes as described in the Notice. If a member of the DMH workforce keeps Psychotherapy Notes, he or she does so as an individual, and is therefore individually responsible for their content, control, protection, access and disclosure, including disclosure pursuant to a court order or as otherwise required by law. All DMH Treatment and Payment information should be kept in the applicable DMH record.

As applicable, the DMH facility must inform the Patient that the request has been granted and provide access as requested (see " Reply To Request To Inspect And/Or Copy", form M-451A, Appendix #10). PHI should be provided in the format requested as allowed by SCDMH policy, unless he or she agrees to a written summary as described in the Notice. If the same PHI is maintained in more than one Designated Record Set or at more than one location, the PHI may only be produced once. If the facility does not maintain the requested PHI, but knows where it is maintained, the facility should inform the individual where to direct the request.

If access is denied, the DMH component must provide a written denial within 30 days of the request (see "Reply To Request To Inspect And/Or Copy", form M-451A, Appendix #10). If the Patient requests a review in writing, the component must designate a licensed health care professional who was not involved in the denial decision to review the denial. Response to the request of review of the denial must be within 30 days of the request for review of the denial.

8. **Patient's Right to Request Amendment to PHI**
After a Patient requests an amendment in writing ("Request To Amend SCDMH Protected Health Information", form M-452, Appendix #11) staff must act on the request in accord with the Notice timelines and procedures. The request must be forwarded to the component director with copy to the local Privacy Officer. The director must designate staff to review the request and take needed action. The request must be reviewed by the designated staff in conjunction with staff originally recording the PHI and by the staff's supervisor(s), who must consult with other staff as needed to determine if an amendment is needed. Any conflict must be resolved by the director. The Patient must be informed of the final decision by a letter substantially similar to the "Model Reply To Request To Amend" (Appendix #12) with a copy of the original "Request", including details of the review and explanation of the approval or denial.

If the request for amendment is approved, after notifying the Patient as noted above and obtaining the Patient's agreement with the proposed amendment, the amendment should

be made, the record flagged to indicate the amendment and the amendment form filed in the record. Staff should also attempt to secure the Patient's permission to notify necessary relevant persons of the amendment. If the Patient refuses, document the attempt to obtain permission in the record prior to giving needed notification.

A request for amendment may be denied if the PHI: was not created by DMH; is not in the Designated Record Set; or the PHI is accurate and complete. If the request is denied, the Patient must be notified in writing as described above indicating: the basis for the denial; that the Patient may submit a one-page written disagreement, stating the basis for disagreement; that the Patient may request that future disclosures of the disputed PHI include the request and the denial; and how the Patient may file a Complaint.

Records must be maintained identifying the PHI in the Designated Record Set that is the subject of the disputed amendment and appended or otherwise linked to the Patient's request for amendment, DMH denial, Patient's statement of disagreement, and any DMH rebuttal. If a Patient submits a statement of disagreement following a denial, subsequent disclosures of the disputed PHI must include the above items.

9. **Patient's Right to Request Accounting of Some PHI Disclosures**
DMH components must log each PHI disclosure that requires an accounting of disclosure using the "Accounting Log Of PHI Disclosures" (paper form M-453, Appendix #13) or "PHI Disclosure Form" (electronic). The accounting must include disclosures by DMH as well as disclosures to a DMH Business Associate. This accounting requirement does not include PHI used or shared before April 14, 2003 or other disclosures described in the Notice. The local Privacy Officer or designee must respond to a Patient's written request, and provide, a copy of the applicable accounting log as described in the Notice (see "Model Reply To Request Of Accounting Log", Appendix #14). However, a Patient's right to receive an accounting log must be suspended if a health oversight agency (HHS) or law enforcement official notifies DMH that providing an accounting would be reasonably likely to impede the health oversight or law enforcement agency's activities and specifying the time for which the suspension is required. DMH must document that statement (including the identity of the agency or official) and temporarily suspend the Patient's right to an accounting for no longer than 30 days, unless a written statement is received from the applicable agency during that time.

10. **Patient Privacy Practice Complaints**
Applicable DMH components must, in coordination with the local Privacy Officer and Patient Advocate, have a process for Patients to make a written complaint about DMH privacy practices or compliance with those practices ("SCDMH Privacy Practices Complaint", form PR-11, Appendix #15) and must document all complaints received and their disposition as described in the Notice. At any time, a Patient has the right to file a complaint with DMH and/or HHS as described in the Notice. DMH must provide records and compliance reports, as required by HHS and otherwise permit access, as requested by HHS, to applicable facilities, records, and other sources of Information, including PHI as needed for an HHS inquiry or investigation pursuant to a Complaint.

DMH component or staff may not intimidate, threaten, coerce, discriminate against, or retaliate against any person for the exercise of rights or participation in any process relating to this Directive, or against any person for filing a complaint with DMH, HHS or other privacy related investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA or state law as long as the action does not involve disclosure of PHI in violation of the regulations, nor require individuals to waive any of their rights under HIPAA or state law as a condition of Treatment or eligibility for DMH services.

11. DMH Privacy Officer:

DMH must designate a DMH Privacy Officer responsible for the development and implementation of DMH privacy practices. Applicable DMH components must designate a local Privacy Officer that advises at the facility level.

12. Training

Each new workforce member must receive Privacy and Security training within 30 days after joining the workforce and annually thereafter. Each workforce member, whose functions are impacted by a material change in this Directive, or by a change in position or job description, must receive the training as described above within a reasonable time after the change becomes effective. All training must be documented and records retained for 6 years.

13. Sanctions and Mitigation of Damages

DMH Human Resources office must document and each DMH component must apply, appropriate DMH employee disciplinary action, for employees who fail to comply with this Directive. Exceptions include disclosures made by employees as whistleblowers, for mandatory reporting or certain crime victims. Each DMH component must have a process to mitigate, to the extent practicable, any harmful effects of unauthorized uses or disclosures of PHI by the component or any of its Business Associates.

14. Security

Per the DMH HIPAA Risk Analysis Policy, each system will be tested once a year by the DMH internal security team and at least once every third year by a third party to verify internal assessment. Problems identified during the assessment will be reported in writing and include a corrective action plan with a copy provided to the local Privacy Officer for follow up and resolution. Reasonable efforts will be made to mitigate and correct identified problems. Unresolved problems must be reported to the DMH Privacy Officer.

Emailing PHI must follow the standards outlined in the Electronic Communications Policy (MED-17-20).

General Guide for Copying or Faxing Protected Health Information

14.1. Post a sign near copy/fax machine similar to the following: "All paper containing Protected Health Information that is no longer needed, including extra copies or sheets that are copied incorrectly, must be shredded immediately, or placed in the large shredding bins."

14.2. Information disclosed should be the minimum necessary to accomplish the intended permitted purpose.

14.3. For fax cover sheets referring to a patient, unless essential for the understanding of the message, de-identify or otherwise limit the identity of the patient.

14.4. Double check phone/addresses prior to sending faxes or e-mails.

14.5. Only send to DMH staff who need the information in doing their DMH job.

14.6. Do not leave PHI documents at the copy/fax machine once the information has been copied or faxed,

Any communications or transmissions that include PHI should identify the intended recipient, the sender (with reply contact information) and include a notice statement substantially similar to the following:

PRIVACY NOTICE: THIS COMMUNICATION IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN SCDMH PATIENT OR OTHER INFORMATION, THAT IS PRIVATE AND PROTECTED FROM DISCLOSURE BY APPLICABLE FEDERAL AND/OR STATE LAW. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT OR RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION OR THE INFORMATION CONTAINING WITHIN IT, IS STRICTLY PROHIBITED AND MAY SUBJECT THE VIOLATOR TO CIVIL AND/OR CRIMINAL PENALTIES. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE, REPLY E-MAIL OR FAX USING THE PHONE NUMBER OR ADDRESS IDENTIFIED IN THIS COMMUNICATION AND DESTROY OR DELETE ALL COPIES OF THIS COMMUNICATION AND ALL ATTACHMENTS.

15. Documentation Requirements:

Applicable DMH components must maintain Directive policies and procedures in written or electronic form as well as written or electronic copies of all communications, actions, activities or designations required to be documented by this Directive, for 6 years from the later of the date of creation or the last effective date.

16. Disclosure of Unidentifiable Information or Information in Limited Data Sets

PHI may be disclosed under the requirements and protocols described in "Unidentifiable Or De-Identified Information" (Appendix #16) or "Limited Data Sets" (Appendix #17).

17. Charges for Copying and Other Expenses Related to Copying and Access to PHI.

As permitted by this Directive, PHI may be disclosed by photocopy or fax. There are no costs to other healthcare providers when copies are provided for purposes of treatment, payment or operations. For other disclosures, a fee to cover costs of reproducing may be charged and collected in advance of providing copies.

17.1. Paper record – For purposes of DMH and this Directive, paper records apply to those facilities that maintain all or a portion of their record on paper. . The standard rate can be calculated and charged as a per page fee only in cases where the PHI requested is maintained in paper form and the individual requests a paper copy of the PHI or asks that the paper PHI be scanned into an electronic format. Per page fees are not permitted for paper or electronic copies of PHI maintained electronically.

17.2. Electronic Record - For purposes of DMH and this Directive, the Outpatient EMR and Inpatient Electronic Health Record (EHR) systems are considered electronic

records systems and electronically maintained PHI, and in calculating costs for copies for patients, the "actual costs" or the "flat fee" rates would be appropriate. Per page fees are not permitted for paper or electronic copies of PHI maintained electronically. The charge is either a flat fee not to exceed $6.50, inclusive of all labor, supplies, and any applicable postage, or based on the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically which is approved by Office of General Counsel.

17.3. When requests for copies are to be provided in electronic format, a PDF version may be provided in lieu of paper copies.

18. Breach Notification

The HIPAA Breach Notification Rule, 45 CFR 164.400-414, requires DMH and DMH Business Associates to provide notification following a breach of unsecured protected health information. A breach is an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of protected health information. The SCDMH Privacy Officer should always be notified of a potential breach by completion of the "HIPAA Incident Report" (form M-454, Appendix #18). Determination will be made if further individual reporting or reporting to Health and Human Services (HHS) or the Media is required. A risk assessment will be conducted to determine if SCDMH or the SCDMH Business Associate can demonstrate that there is a low probability that the protected health information has been compromised, the nature and extent of the protected health information involved, whether the protected health information was actually acquired or viewed, and the extent to which the risk to which the protected health information has been mitigated. When individual notices are required, they must be provided in written form and by first class mail using the "Model Breach Notification Letter SCDMH" (Appendix #19) as a guide. Individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.

19. Decommissioned / Vacated Areas

A Decommissioning Process must be completed whenever a DMH facility, mental health center, or other location is removed from service and vacated, including temporary locations or recreational vehicles or trailers. Procedures should be followed to assure that all electronic and non-electronic forms of Personally Identifiable Information (PII), Protected Health Information (PHI), and other private and confidential information (e.g. employment information, social security numbers) are removed from any DMH occupied space. The process includes completion of the "Clearance Verification for Decommissioned Premises" (form AS-1, Appendix #20) by a Designated Individual Responsible for removing all confidential information. A copy is submitted to and maintained by the Mental Health Center Director or DIS Office of Compliance for DIS facilities.

20. Disclosure to Law Enforcement

Pursuant to South Carolina Code Section 44-22-100 (A)(4), disclosure is necessary to cooperate with law enforcement when there are administrative demands for medical records disclosure. When records are demanded from law enforcement, the Administrative Demand for SCDMH Records (form M-450F, Appendix # 21) should be requested from the demanding law enforcement agency.

21. Violations and Penalties

All violations of this directive must be reported to the applicable person's supervisor. The "HIPAA Incident Report" (form M-454, Appendix #18) is used for all HIPAA incident reporting. DMH employees who make an unauthorized disclosure of PHI, or otherwise violate provisions of this Directive, are subject to disciplinary action in accordance with the DMH Directive Employee Disciplinary Standards . Further, South Carolina law and Federal law provides for penalties for the unauthorized disclosure of PHI ranging from $100 up to $1.5 million per violation and imprisonment. Unauthorized use or disclosure of PHI may also subject the employee to additional civil or criminal liability.

This Directive with referenced "Notice of Privacy Practices" and Appendices, replaces the DMH Privacy Practices Directive 837-03. This Directive is effective November 1, 2021.

Kenneth Rogers, MD
State Director
Effective November 1, 2021

APPENDIX TO OMH PRIVACY PRACTICES DIRECTIVE

1) Notice Of Privacy Practices, M-010

2) SCDMH Privacy Practices Acknowledgement and Agreement, HRS-2

3) Consent To Examinations And Treatment, C-107

4) Model Notice Of Privacy Law

5) Disclosures In Legal Proceedings

6) Authorization To Disclose OMH Protected Health Information, M-450D

7) Authorization to Disclose Protected Health Information to OMH, M-450E

8) Model Notice Prohibiting Re-Disclosure

9) Request To Inspect And/Or Copy OMH Protected Health Information, M-451

10) Reply To Request To Inspect And/Or Copy, M-451A

11) Request To Amend OMH Protected Health Information, M-452

12) Model Reply To Request To Amend

13) Accounting Log Of PHI Disclosures, M-453

14) Model Reply To Request For Accounting Log

15) OMH Privacy Practices Complaint, PR-11

16) Unidentifiable Or De-Identified Information

17) Limited Data Sets

18) HIPAA Incident Report, M-454

19) Model Breach Notification Letter SCDMH

20) Clearance Verification for Decommissioned Premises, AS-1

21) Administrative Demand for OMH Records, M-450F