



State of New Jersey

DEPARTMENT OF HUMAN SERVICES
DIVISION OF MENTAL HEALTH AND ADDICTION SERVICES
222 SOUTH WARREN STREET
PO Box 700
TRENTON, NJ 08625-0700

CHRIS CHRISTIE
Governor

ELIZABETH CONNELLY
Acting Commissioner

KIM GUADAGNO
Lt. Governor

LYNN A. KOVICH
Assistant Commissioner

DIVISION OF MENTAL HEALTH AND ADDICTION SERVICES

ADMINISTRATIVE BULLETIN TRANSMITTAL MEMORANDUM

DATE ISSUED: April 27, 2004

REVISED EFFECTIVE DATE: May 1, 2015

SUBJECT: Enactment of Amendments to the Division of Mental Health and Addiction Services' (DMHAS) Administrative Bulletin 3:28 - Privacy and Security of Protected Health Information

Attached is the newly amended Administrative Bulletin (AB) 3:28 which continues to address confidentiality, privacy and security of consumer protected health information (PHI). This newest version of the AB replaces all earlier versions of AB 3:28. The purpose of this memorandum is to highlight the amendments and modifications to AB 3:28 and present a focused summary of noteworthy major and minor changes.

The AB provides that information about consumers be kept confidential whether that information is in the form of paper or electronic documents, verbal communications, electronic transmissions or photographs. HIPAA requires that Division of Mental Health and Addiction Services (DMHAS) facilities create a designated record set, which contains confidential information and which requires consumer authorization for most access and release to others. DMHAS staff must safeguard information about consumers, including their identity and any information that exists in any form outside of the designated record set. All staff and volunteers must be trained in confidentiality practices. Other noteworthy changes to AB 3:28 include:

1. HITECH

The newly amended AB 3:28 fully adopts the statutory privacy mandates of the *Health Information Technology for Economic and Clinical Health Act* (HITECH). The AB requires compliance by the Division and its employees with all statutory HITECH requirements, including requirements relating to: (1) electronic records, (2) electronic transmissions and (3) Business Associate Agreements.

2. Privacy Officer Access to Risk Incident /Investigative Reports

Under Section IX of AB 3:28, incident reports must be completed for all situations where there are PHI breach allegations. Additionally, Privacy Officers are permitted full access to hospital Risk Management investigation and incident reports relating to privacy breaches.

3. Fees for Copies of Medical Records

AB 3:28 adds Section XIII entitled *Access To Records By Clients*. Subsection D of this section of the AB permits the hospital to charge a monetary fee for photocopies of medical records. The fees specified are identical with fees permissible in HIPAA and HITECH and will unify Division hospitals by providing a standardized photocopy rate for medical records that is in accord with the federal statutes. In accordance with federal statutes, AB 3:28 limits the amount that can be charged to a patient or the patient's representative for hospital records to \$200.00.

4. Notifications in the Event of a Breach

The amended AB 3:28 requires that notification of a PHI breach be made to consumers whose PHI is wrongly disclosed. Section XIX entitled *Sanctions and Mitigation* brings the AB in accord with HIPAA requirements mandating notification of PHI breaches to the affected consumers. These changes can be found in Subsection C of Section XIX.

5. Psychotherapy Notes

AB 3:28 - Section VII – Subsections E and F (Disclosure To Third Party) clarifies that records which meet the HIPAA definition of psychotherapy notes should not be stored or filed with the designated medical record set. Psychotherapy notes are not part of the designated medical record set and shall be filed in a secure location separate from the designated medical record set.

6. Security Officers

For HIPAA compliance purposes, the DMHAS and hospital information technology directors shall serve as the facility HIPAA security officers. HIPAA security officers are responsible for assuring the facilities take adequate steps to secure sensitive information from those who do not have a right to see it.

7. Privacy Officers

HIPAA requires designated Privacy Officers for the DMHAS and its individual hospitals. The Privacy Officer is responsible for assuring that policy and practice are in line with the law. The Privacy Officer will also ensure that training in confidentiality and the mandates of AB 3:28 are available and accurate, and that all complaints made regarding confidentiality are handled in a prompt, thorough and professional manner.

Currently, Privacy Officers in the DMHAS are:

Central Office	Lisa Ciaston and Jeff Nielsen
Ancora Psychiatric Hospital	Charlene Ruberti
Trenton Psychiatric Hospital	Manoj Thomas
Ann Klein Forensic Center	Mirelle Jeanmisere
Greystone Park Psychiatric Hospital	Maria Mancini

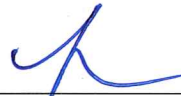
The Department of Human Services' (DHS) Privacy Officer is Bonny Fraser.

Any change in this list will be updated on the Department/DMHAS website.

Finally, please advise all staff that a breach of HIPAA requirements can lead to monetary penalties and sanctions against the State and individual staff members. In extreme circumstances involving intentional violations, criminal prosecution may be sought along with Administrative employment action.

If you have any questions about this policy, please see your Privacy Officer. The new, amended AB 3:28 is effective May 1, 2015.

Attachment



Lynn A. Kovich
Assistant Commissioner

DIVISION OF MENTAL HEALTH AND ADDICTION SERVICES

ADMINISTRATIVE BULLETIN 3:28

DATE ISSUED: April 27, 2004

Revised Effective Date: May 1, 2015

SUBJECT: PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

I. PURPOSE

To provide a standardized guideline consistent with current Federal and State laws and regulations, Department Orders and Division Bulletins concerning the confidentiality of client health information.

II. SCOPE

This Bulletin applies to all Division of Mental Health and Addiction Services' (Division) staff and all Department of Human Services (Department) Central Office staff who have access to Protected Health Information (PHI) of Division clients, including the records kept at all hospitals and administrative units operated by the Division.

III. AUTHORITY

Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), the HIPAA Privacy & Security Rule (45 C.F.R. Parts 160 & 164), as amended pursuant to the HITECH (Health Information Technology for Economic and Clinical Health) Act.

N.J.S.A. 30:4-24.3
N.J.S.A. 2A:62A-16
N.J.S.A. 26:5C-8
42 CFR Part 2
Administrative Order 2:01

IV. STATEMENT

Division and Department employees who create or have access to client PHI have an ethical and legal responsibility to maintain the privacy and security of all such information, whether it is communicated or maintained in the form of computerized, electronic, or paper records or verbal communications. This Bulletin sets forth guidelines for members of the Division workforce regarding clients' access to their treatment records, the disclosure of information within and outside the treatment setting, and the security measures staff must take to prevent unauthorized disclosures of client PHI.

V. RESPONSIBILITY

- A. Employees shall access only the minimum PHI necessary: (1) to perform assigned tasks responsibly; (2) when required by hospital policies and practices; (3) for maintaining the privacy of information about clients that they need to use to do their jobs; (4) for destroying information that they no longer need in accordance with State laws, including the State record retention schedule; and (5) for reporting any inadvertent release or security problem to the appropriate Privacy Officer.
- B. Privacy Officers are responsible for: participating in training offered by the Department's Privacy Officer and for assuring that confidentiality training is available and accurate for current staff and new staff as they are hired; for working with supervisors to mitigate any unauthorized access or release by their direct reports; for assuring that hospital and office procedures and practices are compliant with privacy standards; and for resolving disputes about access and referring complaints of privacy violations to the Department's Privacy Officer.
- C. Business Managers at state psychiatric hospitals, and Division program analysts in the regions, in consultation with the Privacy Officers, are responsible for assuring that business associates performing non-clinical services under contract with the Department or any of its facilities which in the course of performing that contract have access to client PHI are identified, and that the contracts contain appropriate language to assure that each contractor is aware of its obligation to maintain privacy and security of client information, including compliance with the breach provisions of HITECH.
- D. Discipline heads at the hospitals and Division regional coordinators are responsible for assuring that affiliation agreements contain appropriate language to assure that the affiliates are aware of their obligations to maintain privacy and security of client information and client PHI.
- E. Human Resources Directors are responsible for maintaining, for each employee, and any contracted employees a personnel file which includes a copy of the confidentiality statement given to each employee or contracted employee.
- F. Each hospital and each regional office shall implement this Bulletin.

VI. DEFINITIONS

- A. **Authorization** is the signed documentation which evidences that a client or client's guardian has consented to the disclosure of PHI in the designated record set to an external third party. An authorization may be revoked by the signer except to the extent that the staff or another party has taken action in reliance on it. Every authorization shall state either a date or event on which the authorization shall expire, and no authorization shall be honored after that date or event.

- B. **Breach** is an unauthorized acquisition, access, use, disclosure of unsecured PHI in a manner not permitted by the HIPAA Privacy Rule that compromises the PHI.
- C. **Business associate** means, with respect to a person or affiliating agency, an entity outside the Department that, on behalf of the Division or a state psychiatric hospital, performs or assists in the performance of:
1. A function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, data storage, data processing or administration, utilization review, quality assurance, billing, benefit management, therapeutic services; or
 2. Any other function or activity described by this bulletin where the provision of the service involves the creation or disclosure of PHI from the hospital to the business associate.
- A person or organization that is independently required to conform to the state and federal privacy standards referenced in this bulletin is not required to be a business associate.
- D. **Covered Entity** means an organization or person required by law to comply with HIPAA (45 CFR parts 160 & 164).
- E. **Designated record set** means a group of records maintained by a psychiatric hospital that is used, in whole or in part, to make treatment decisions about individuals and is contained in the medical records and/or billing records about clients maintained by or for the Division or a state psychiatric hospital.
- F. **Disclose** means release, transfer, provide, give access to, or divulge in any other manner any protected health information about a consumer.
- G. **Personal Representative** of a client means a legal guardian or mental health care representative when an advance directive for mental health or health care is operative, or a person who has a valid power of attorney, durable power of attorney, or medical proxy executed by a consumer who has no legal guardian.
- H. **Protected Health Information (PHI)** means any record that describes or discloses the past, present, or future physical or mental health or condition of a client; the provision of health care to a client; or the past, present, or future payment for the provision of health care to a client. The fact that a person is a client of the mental health system is PHI. Information that has been de-identified or which is included in a limited data set for purposes of research in accordance with research protocols and Administrative Order 2:01 is not PHI. Restrictions on disclosures and uses of PHI apply to clients during and after their lifetime.
- I. **Privileged communications** are statements made to a person who is licensed in the State of New Jersey to practice law, psychology, medicine, nursing, or marriage counseling; or who is a licensed clinical social worker; or who is a priest or minister, or a victim counselor as defined at NJSA 2A:84A-22.13, as part of a client-therapist relationship.

- J. **Psychotherapy notes** are privileged communications recorded by a therapist that are separated from the rest of the client's clinical record, but do not include: medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis or treatment made for or provided to another treating professional. Generally, state psychiatric hospitals do not create or maintain psychotherapy notes. Psychotherapy notes are not part of the designated records set.
- K. **Record** means any item, collection, or grouping of information that is maintained, collected, used, or disseminated by or for the Division. A government record, or public record, as defined in P.L. 2001, c. 404, is a record made, received, or maintained by a government employee that is not exempt from disclosure under that or any other law. Individual clients' clinical and financial records are never government/public records and may only be disclosed in accordance with this bulletin. See A.B. 3:24 for disclosure of public records. See A.B. 3:27 for release of records to New Jersey Disability Rights and the Mental Health Advocacy unit of the Public Defender.
- L. **Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a client; or the referral of a client for health care from one health care provider to another.
- M. **Use** means, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within the Division or the Department or with business associates of any of the Department's functional units.
- N. **Workforce** means those persons who work with or on behalf of clients of DMHAS at a state psychiatric hospital or other state-owned office or facility to provide treatment, arrange payment, or operate the hospital, whether paid by DMHAS or paid at all, and includes employees of the Department of Human Services, persons who are employed by another employer who provide or coordinate treatment for hospital patients, and appropriately screened and trained volunteers who are supervised by paid Department staff. The designation of a person as part of the workforce for purposes of privacy does not render that person a State employee for any other purpose.

VII. DISCLOSURE TO A THIRD PARTY

- A. Division employees are permitted to disclose PHI:

- 1. WITH CLIENT AUTHORIZATION:

- Any information in the record may be disclosed upon the execution or receipt of a consumer's written authorization, except with respect to information about treatment of and subject to Federal and State limitations and restrictions on authorization to release HIV status and drug or alcohol treatment information. For this purpose, consumer shall mean:

- a. An adult consumer who does not have a legal guardian; or
 - b. The personal representative of a consumer; or
 - c. An incompetent adult's guardian or the parent or guardian of a minor who is either an involuntary inpatient or is under 14 years of age; or
 - d. A consumer between the ages of 14 and 17 who is voluntarily receiving mental health treatment; or
 - e. With respect to those records, a minor who has consented to his or her own treatment for drug use, drug abuse, alcohol use, alcohol abuse, sexual assault, or venereal disease (see sections VII C & D); or
 - f. With respect to HIV records, a minor over the age of 12 who has consented to his or her own treatment (see section VII E).
2. PURSUANT TO A COURT ORDER:
- a. Except for psychotherapy notes (see section VII F) and records of HIV status (see section VII E), pursuant to an order of a New Jersey court (municipal or state) in which the court has determined that disclosure is necessary for the conduct of proceedings before it and that failure to make such disclosure would be contrary to the public interest.
 - b. A subpoena or out of state order may not be sufficient authority to release PHI, and should be referred to the Office of the Legal and Regulatory Liaison.
3. UNDER THE OTHER FOLLOWING CIRCUMSTANCES WITHOUT AUTHORIZATION OR A COURT ORDER:
- a. A member of the workforce engaged in treatment, payment, or operations, including a member of the state hospital's workforce, a Division or Department employee, or an employee of a community mental health agency that is under contract with the Department or Division to provide post-discharge treatment, or any DMHAS contracted administrative entity for the management of program services is entitled to use only the minimum necessary PHI (see G., below) to carry out treatment, payment, or health care operations.
 - b. The Human Services Police may access PHI in accordance with the procedures in A.B. 3:10A.
 - c. A Business Associate that has executed the appropriate agreement is entitled to any records made or maintained by the hospital or Division that are necessary to carry out the functions of the contract or agreement.

- d. To the extent the disclosure would not, as documented by a treating clinician, cause harm to the consumer or another person, a current consumer or his or her personal representative is entitled to inspect and obtain a copy of the clinical or financial records in the consumer's designated record set under the following conditions:
 - i. Consumers must be provided a safe and private place to meet to discuss their records with their attorneys or other personal representative or physician.
 - ii. The treatment team may require that a designated mental health professional be present when a consumer first examines a clinical record to aid in the interpretation of information in the record, if the treatment team documents that unaccompanied disclosure would cause harm to the consumer.
 - iii. If any such records are kept electronically, the consumer must be offered the opportunity to inspect or receive copies in an electronic format.
- e. A consumer's PHI can be shared with a family member, relative, friend, personal physician or attorney of the current consumer provided the relationship is verified and the treatment team determines the disclosure is in the best interest of the consumer.

If the consumer objects to the sharing of PHI then no information shall be disclosed.

In emergency situations, if the inquirer has been identified by the consumer as the emergency contact or next of kin; or is known to the staff to be a family member, relative or friend of the consumer and the disclosure would be in the opinion of the team in the best interests of the consumer, a team member can inform the inquirer of the consumer's location and general medical condition without giving the consumer the opportunity to object to the disclosure.

- f. A person who formerly received services from a facility is entitled to inspect or obtain a copy of his or her clinical or financial records. If the records are available in an electronic format, the person must be offered the opportunity to inspect or receive copies electronically.
- g. The medical staff of a hospital outside the Department or a medical consultant retained by the facility which has assumed temporary medical responsibility for the consumer, or any physician or another covered entity in an emergency situation may have access to PHI to prevent death or serious bodily harm to the consumer.
- h. A person or persons not employed by the Department but designated by the Commissioner to fulfill his or her responsibilities under law may access

PHI as necessary to meet those responsibilities, including but not limited to:

- i. persons participating in a Professional Standards Review Organization; and,
 - ii. authorized inspectors from The Joint Commission, the Federal Department of Health and Human Services, or the State Department of Health, with appropriate assurances as required by HIPAA.
- i. The Division shall disclose relevant PHI about a minor to the Division of Child Protection and Permanency (DCP&P) in the Department of Children and Families, in connection with a current investigation of whether the minor has been abused or neglected, where DCP&P has requested pertinent records of the minor.
 - j. The Division shall disclose PHI to staff of the Ombudsman for the Institutionalized Elderly (OIE) upon presentation of proper identification, where OIE has made a proper request and the consumer is 60 years of age or older.
 - k. PHI shall be provided by a hospital to an authorized representative of a county adult protective services provider with proper proof that a current inpatient consumer has been declared a vulnerable adult. This information will normally be limited to the location of the consumer.
 - l. PHI shall be disclosed to any person (or the person's insurance carrier) whom a consumer or former consumer or his or her estate has sued for compensation or damages for personal injuries or death resulting from personal injuries, either under New Jersey Worker's Compensation or in a civil suit.
 - m. PHI shall be disclosed to county physicians as needed to certify the cause of death in a state psychiatric facility as required by NJSA 30:4-103, and 30:4-105. When a consumer dies, Division employees may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the consumer, such as Disability Rights New Jersey (DRNJ) or another person responsible for the disposition of the consumer's body.
 - n. Physicians shall disclose, to fulfill their obligation under NJSA 39:3-10.4, to the Director of the Division of Motor Vehicles, the name of anyone who is 16 years old or older and who is subject to recurrent convulsive seizures or similar conditions. To the extent possible, a physician required to so report shall not disclose that the consumer is a recipient of mental health services.
 - o. A hospital shall disclose to the State Department of Health PHI about infections and contagious diseases to the extent required by law.

- B. Information about drug or alcohol abuse or treatment may only be released by court order or proper authorization of the consumer or guardian that complies with 42 C.F.R. Part 2.
- C. An authorization to disclose information about treatment to which a minor of any age consented and which concerns drug use, drug abuse, alcohol use, alcohol abuse, sexual assault, or a sexually transmitted disease may be executed by the minor or by the parent or guardian with the minor's assent.
- D. Information about a consumer that would reveal HIV status is protected by state law (N.J.S.A. 26:5C-8) from disclosure without specific authorization or a court order that conforms to the standards in that statute.
 - 1. A court order that would require the release of HIV status should be referred to the Office of the Legal and Regulatory Liaison.
 - 2. If an authorization will permit the release of information identifying a consumer's HIV status, and if the consumer is legally incompetent or deceased, the following persons can authorize release:
 - a. The consumer's executor, administrator of the estate, or authorized representative,
 - b. The person's spouse, guardian, or primary caretaking partner or, if none, another member of the person's family;
 - c. If a deceased person has none of the representatives described above, the Commissioner of Health.
- E. Generally, no records meeting the definition in HIPAA of psychotherapy notes are kept in Division hospitals. If, however, they do exist and their disclosure is requested, psychotherapy notes may only be accessed without the consumer's specific authorization under the following circumstances:
 - 1. To carry out treatment, payment, or health care operations;
 - 2. By the originator of the psychotherapy notes for use in treatment;
 - 3. By hospital personnel in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
 - 4. By the Department to defend a legal action or other proceeding brought by the consumer.
- F. Minimum necessary disclosures of PHI
 - 1. For any type of disclosure that a hospital or other division unit makes on a routine and recurring basis, it must implement policies and procedures that

limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of this disclosure.

2. For non-routine disclosures, employees must:
 - a. Limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and
 - b. Review requests for disclosure on an individual basis in accordance with such criteria.
3. A hospital may rely, if such reliance is reasonable under the circumstances, on the representation of a public official or licensed health care professional that the information requested is the minimum necessary for the stated purpose.

G. Duty to warn

1. A licensed clinician may be required by state law to breach confidentiality of otherwise privileged communications with a consumer when the consumer has communicated, or the clinician can discern, a clear intention to harm him or herself or another identified person.
2. A clinician who makes such a disclosure within the standards in N.J.S.A. 2A:62A-16 will not be sanctioned by the Division for a failure to follow the standards in this Bulletin.

VIII. AUTHORIZATIONS

- A. Where a consumer's authorization is required to disclose PHI, the authorization shall be written in plain language and shall contain:
 1. The name of the consumer;
 2. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
 3. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
 4. The name or other specific identification of the person(s), or class of persons, to whom a Department employee may make the requested use or disclosure;
 5. An expiration date or an expiration event that relates to the consumer or the purpose of the use or disclosure; unless a different expiration time or event is stated on the authorization, it expires on the 90th day after it is signed;
 6. A statement of the consumer's right to revoke the authorization in writing, statement that this right is absolute except to the extent that the treating facility has already acted in reliance on the authorization, or to the extent that

the information may be legally required to be released for insurance purposes, and a description of how the consumer may revoke the authorization;

7. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient;
 8. Signature of the consumer and date on which it is signed; and
 9. If the authorization is signed by a personal representative of the consumer, a description of the representative's authority to act for the consumer.
- B. A statement that the treatment cannot be conditioned on signing the authorization.
 - C. If an authorization is submitted that does not contain the information required by this section, the recipient of the request shall advise the requestor that the form is inadequate and shall send a compliant form to the requestor. No PHI shall be released until the properly signed form is received.
 - D. The Division employee who releases information pursuant to an authorization shall document and retain the authorization in accordance with the hospital or Division's procedures for at least six (6) years.
 - E. An authorization shall be honored if the staff person receiving the authorization is satisfied, through personal knowledge or acknowledgement by a notary, that the signature is valid.
 - F. If there is no signature and the consumer is present, a disclosure can be authorized by the Privacy Officer if it can reasonably be inferred from the circumstances, based on the exercise of professional judgment that the consumer does not object to the disclosure.

IX. PRIVACY OFFICERS

- A. Each administrative unit of the Division, including Central Office and each facility, shall have a Privacy Officer, designated by the Assistant Commissioner or CEO, who shall receive training and guidance from the Department's Privacy Officer on the implementation of the standards in this Bulletin and in Administrative Order 2:01.
- B. If access to PHI is denied pursuant to this policy, the Privacy Officer will arrange to have the denial reviewed by a licensed health care professional who did not participate in the original decision to deny the request. The Privacy Officer will decide whether access should be granted, and inform the requestor of his or her right to appeal that decision to the Department's Privacy Officer.

- C. If a consumer believes that an employee has violated his or her rights to privacy under this Bulletin, and communicates that belief to any Division employee, that employee shall document the complaint and forward it to the facility's Privacy Officer. An incident report shall be completed and the incident investigated pursuant to existing risk management procedures, and the incident report, the investigation report, and any documentation of a breach of privacy shall be made available to the Privacy Officer, who shall ascertain what if any privacy right was violated. The Privacy Officer shall take whatever measures are appropriate to stop any further unauthorized disclosure. A copy of the Privacy Officer's conclusions shall be forwarded to the alleged offender's supervisor, who will impose appropriate discipline if the violation is substantiated, and to the consumer, and to the Department's Privacy Officer, who shall monitor the disciplinary and reporting processes if privacy rights were violated. The Privacy Officer shall advise the consumer of his or her right to complain or appeal to the US Department of Health and Human Services and the Department if unsatisfied with the outcome.
- D. All privacy officers shall participate in Departmental training on the issues of confidentiality and security, and shall advise the unit or hospital's trainers on delivery of mandatory training required by federal and state standards.
- E. The privacy officer shall ensure that policies and systems exist to enable staff to keep records of disclosures and to make accountings of disclosures to consumers who properly request them.

X. NOTICE OF PRIVACY PRACTICES

A consumer has a right to adequate notice of the uses and disclosures of protected health information that may be made by the Division, and of the consumer's rights and the Division's legal duties with respect to protected health information.

- A. Initial Distribution: Psychiatric hospitals must provide to each patient in treatment at the time this Bulletin takes effect or upon admission to the facility, or as soon as practicable after admission, a copy of the Department's current Notice of Privacy Practices that explains the Department's privacy practices, including the uses and disclosures it will make of PHI, the right of the consumer to amend the record, and the right to receive copies of records created and an accounting of disclosures made by Division employees. The hospital will make a good faith effort to obtain the signature of the consumer acknowledging receipt of the notice.
- B. Changes to Privacy Practices: Any time the Department's privacy practices change or are altered by any change in law, the facility will advise any current consumers of the change at the time of the first contact for treatment after the change takes effect.
- C. Posting: Privacy Officers shall arrange for the appropriate posting of the Notice of Privacy Practices in public lobbies and in patient living areas.

XI. CONFIDENTIALITY STATEMENTS

Each employee, volunteer, intern, or other person in the workforce of the Division or a Division facility will receive, upon employment or at the time this Bulletin takes effect, a statement advising the person of the importance of medical privacy as it relates to his or her work for the Department. The statement will be filed in his or her personnel or supervision file.

XII. BUSINESS ASSOCIATE AGREEMENTS

- A. Every contract or affiliation agreement between a Division facility or the Division and a business associate that is required under the contract to have access to consumer PHI shall include language approved by the Department that will establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements contained in that addendum.
- B. Violations of any business associate agreement shall be promptly reported to the Department's Privacy Officer.

XIII. ACCESS TO RECORDS BY CONSUMERS

- A. Consumers have a right, subject to the exceptions in Section B, to access and obtain a copy of the PHI about them that is contained in a designated record set maintained at a Division facility.
- B. A consumer does not have a right to see or copy
 - 1. Psychotherapy notes.
 - 2. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding.
 - 3. PHI prohibited from release by a specific Federal or State law or limited by a court order or a prior agreement with the consumer.
 - 4. Information obtained from a source other than another health care provider that was obtained under the condition of anonymity, if the disclosure would identify the source.
 - 5. Information that would, if disclosed to the patient, would likely cause harm to the patient or someone else, as documented by a licensed health care professional.
- C. If an information request is denied under XIII B.5., the patient shall be informed that the denial is reviewable by the Privacy Officer. A Privacy Officer receiving such a review request shall obtain the opinion of a licensed health care

professional designated by the CEO or Assistant Commissioner who was not involved in the original decision to deny access.

- D. The hospital shall charge a monetary fee for photocopies of medical records as follows:

\$0.75 per page (for the first 10 pages),
\$0.50 per page (for pages 11 through 20)
\$0.25 per page (thereafter)

The maximum photocopy fee that can be charged by the hospital is \$200.00.

The hospital may charge a search fee of \$10.00 per request for photocopies of medical records.

The hospital is permitted to charge for actual costs of mailing medical records.

Consumers not able to afford copies of their medical record will be provided one copy of desired records when said request is made in writing.

XIV. AMENDING PROTECTED HEALTH INFORMATION

- A. A consumer may request that a Division facility or unit accept an amendment to his or her designated record set. That request may be submitted on the Department's Request for Amendment form to the Privacy Officer of the facility whose record s/he seeks to amend. Unless the request is denied for one of the reasons in this section, the Privacy Officer will cause the amendment to be made a part of the designated record set for that consumer within 60 days of the request, shall notify the consumer that the amendment has been accepted, and shall, with proper authorization, notify anyone the consumer has identified or of whom the Privacy Office knows who has a copy of the unamended record.
- B. No part of a record shall be destroyed pursuant to this section.
- C. A request to amend the record shall only be denied if the record the consumer seeks to amend:
1. Was not created by the Division or any of its workforce, unless the consumer shows that the entity that created the record is not able to accept an amendment directly; or
 2. Is not part of the designated record set; or
 3. Would be excluded from disclosure to the consumer under this policy; or
 4. Is accurate and complete.
- D. A denial shall, within 60 days of the request, be communicated to the consumer in writing on a copy of the consumer's request. The denial shall cite the reason for denial and the right of the consumer to submit a statement to the Privacy Officer describing the reason for the desired amendment and to have the

statement and the request, with the denial, filed as part of the consumer's designated record set. The denial shall also advise the consumer of his or her rights to file a complaint pursuant to this policy. (See section IX. C.).

XV. ACCOUNTING OF DISCLOSURES

- A. Each facility and administrative unit will maintain a database of the following disclosures of PHI for six (6) years after each disclosure:
1. To a public health authority that is authorized by law to collect information for the purpose of preventing or controlling disease, injury or disability;
 2. To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;
 3. To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, to the extent required by law;
 4. To a health oversight agency for oversight activities authorized by law, including audits; civil, administrative or criminal investigations; inspections; licensure or disciplinary actions (i.e. Board of Nursing, Ombudsman for the Institutionalized Elderly); civil, administrative or criminal proceedings or actions; or other activities necessary for appropriate oversight of: (i) the health care system; (ii) government benefit programs for which health information is relevant to beneficiary eligibility; (iii) entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards (i.e., The Joint Commission, CMS, Medicaid, Department of Health); or (iv) entities subject to civil rights laws for which health information is necessary for determining compliance;
 5. In the course of any judicial or administrative proceeding, except those proceedings that are part of hospital operations.
 6. As required by law including laws that require the reporting of certain types of wounds or other physical injuries;
 7. Pursuant to a court order or court-ordered warrant, a grand jury subpoena; or an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law
 8. To a law enforcement official either based on the official's request for Protected Health Information or on the covered entity's own initiative;
 9. To a coroner or medical examiner to assist such official in authorized duties;
 10. To an organ procurement organization for organ, eye or tissue donation purposes.

11. Pursuant to a waiver of the authorization requirement for the use and disclosure of PHI for research purposes; for research related to deceased individuals; or to develop a research protocol or for other similar purposes preparatory to research.
 12. To a third party to prevent a serious threat to health or safety but without releasing the location of the warned person;
 13. To appropriate U.S. or foreign military command authorities regarding an individual who is a member of U.S. or foreign armed forces;
 14. To authorized federal government officials for the provision of protective services to the President of the United States, foreign heads of state and certain other government officials and to conduct investigations related to such protective services;
 15. As authorized by and to comply with the workers' compensation law.
- B. Division facilities need not enter into the database a record, if any exists, of the following uses or disclosures of PHI:
1. To carry out Treatment, Payment and Health Care Operations, unless such records are kept and disclosed electronically
 2. To the patient;
 3. Incidental disclosures;
 4. Pursuant to an authorization;
 5. For the directory or census or other registry; or
 6. Any use or disclosure that occurred prior to April 14, 2003.
- C. A consumer or his or her personal representative may request an accounting of all accountable disclosures of the consumer's PHI by submitting a completed Request for Accounting Form to the Privacy Officer.
- D. Each facility or administrative unit shall assure that a consumer's request for an accounting is processed within 60 days and the accounting is given to the requester.

XVI. EXPUNGEMENT OF RECORDS

- A. When a facility receives a court order pursuant to N.J.S.A. 30:4-80.8 through 80.11 directing the expungement of records pertaining to the commitment or institutionalization of a former inpatient consumer, the facility shall take the following actions:

1. The records of the consumer named in the order shall be removed from the general closed files and placed in a separate locked file. Permission to gain access to these files can only be given by the Chief Executive Officer or designee.
2. A notation shall be placed on the front of each such record indicating that the record pertaining to that consumer has been expunged.
3. A notation shall be made on the appropriate facility master list of current and former consumers to indicate the consumer's records have been expunged.
4. Where a record of the person's hospitalization is contained in any database maintained by the hospital, Division, or Department, the record shall be removed from the database to a separate electronic file identified by the former patient's name and patient number.
5. No expunged record or information record directly or indirectly identifying such a person as a former patient may be disclosed by any person, unless the former consumer requests disclosure or is readmitted to any Division facility, in which case the record may be made available to the admitting facility.

XVII. PRIVATE COMMUNICATION REGARDING PATIENTS AND CONSUMERS

Each Division component must have in place appropriate administrative, technical, and physical safeguards to protect the physical security of oral, written and electronic forms of PHI. Although incidental disclosures may occur, staff is expected to take action to minimize this risk. Hospital and Division personnel shall undertake regular assessments of their security procedures relative to PHI. Employees who are terminated or resign shall be required to return keys and access card and tokens, and measures shall be taken to assure that no former employee can access PHI.

A. Oral Communication

1. Staff is expected to use a normal, quiet work tone in telephone conversations.
2. Staff is to ensure that discussions of PHI are not overheard by third parties that do not have a need to know, including discussions in individual rooms, hallways, waiting areas, day rooms and other common areas, on or off-duty.
3. Staff is not to discuss PHI with anyone who does not have a need to know.
4. Staff must be careful when discussing PHI in a consumer's living or treatment space when visitors are present.

5. Whenever possible, PHI should be discussed in private in a conference room or an office with a door that is closed. Precautions should be taken to ensure that confidentiality is maintained at all times.

B. Written Communication

1. Consumer records should be filed in locked cabinets or rooms, when possible. If consumer records are not secured in locked areas, records should be maintained in an opaque folder or binder when not in use or turned over on a desk to prevent disclosure, returned to a locked file cabinet or drawer, or stored in a locked office or file room.
2. Post documents that contains PHI on inside walls.

C. Electronic Communication, including electronic mail.

1. All documents, databases, and other electronic files containing PHI are to be maintained on the network in accordance with security and information technology policies set at the Department and Division levels.
2. Turn computer screens inward, away from flow of traffic.
3. The screen should be minimized, obscured by a password-protected screen saver or the monitor turned off when not in use.
4. Passwords (access codes) are to be unique to each user. Passwords should not be shared without authorization. Passwords should not be given to others, including support staff, to access records.
5. Electronic transfer of PHI is to be used only as necessary, and is to be transferred only within the internal network. No PHI transferred via the internet unless PHI is secured.

D. Facsimile Machines

1. When sending a document, call the intended recipient to alert him or her it is being sent.
2. Use a transmittal sheet that contains a HIPAA warning on each document sent (not each page of the document).
3. The transmittal sheet should have the name of the intended recipient.
4. The sheet should not have any individual-identifying information, including the name of the individual receiving services.
5. There should be a designated area for documents to be kept while awaiting pick-up.
6. Destroy any unused documents.

E. Photocopy Machines

1. When copying documents with individual identifying information, a staff member shall always be present.
2. Destroy any unused documents.

F. Printers

1. A cover sheet with the name of the staff member who produced the document should be the first page if a shared or network printer is used.
2. No information regarding individual receiving services shall appear on the cover sheet.
3. Destroy any unused documents.

G. Destruction of Documents

1. When possible, a paper shredder should be used.
2. Documents may be put in a non-public area to be shredded if there is a HIPAA warning that the material cannot be handled by unauthorized individuals.
3. Manual shredding is acceptable. When manually shredding the staff shall determine that no PHI can be readily retrieved.

H. Visitors

1. Each office and facility building shall have a designated visitor area.
2. There shall be a notice of privacy practices posted in each visitor area.
3. Visitors shall be escorted to the intended meeting place.

XVIII. TRAINING

- A. All employees who handle PHI shall be trained as appropriate in privacy and security standards, and documentation of training by business associates of their employees may be required as part of the contract process.
- B. All new employees shall have as part of their new employee orientation, training on the policies and procedures pertaining to privacy and security of PHI.
- C. Privacy Officers, Quality Assurance Directors, Human Resource Directors, and Training Coordinators shall cooperate to ensure that training occurs and is documented for each employee.

XIX. SANCTIONS AND MITIGATION

- A. Noncompliance with this Bulletin is a violation of Division policy and sanctions pursuant to Administrative Order 4:08 shall be imposed on employees who knowingly or recklessly breach security and privacy of PHI. In addition, there are federal penalties for breaches of some provisions. There shall be no retaliation against an employee who reports a violation of security or privacy standards by another employee or a business associate.
- B. Wherever possible, if there is a breach of privacy or security of confidential information, or if there is a founded complaint by a consumer, either within the workplace or by a business associate or another covered entity, each employee is responsible, within his or her job function, to mitigate any damage caused by such breach. Mitigation may include retrieving information, instructing recipients to destroy information, reprogramming information systems, moving fax machines or computer terminals, restricting access to information, or adopting other new practices designed to reduce the likelihood of a similar future breach.
- C. In case of a breach by the Department or any employee of the Department, or by any business associate of the Division or the Department, notice of the breach must be given to the subject of the wrongly disclosed or used PHI and to the Department of Health and Human Services. In addition, if a wrongful disclosure is made that affects more than 500 residents of the State, the media must be notified that the breach occurred, through the Department's Office of Public Affairs.

XX. EFFECTIVE DATE

This Bulletin is effective May 1, 2015.



Lynn A. Kovich
Assistant Commissioner