

**Orrville Hospital Foundation, dba
Dunlap Community Hospital and its
Affiliated Entities
(Collectively "Dunlap")**

**HIPAA Privacy and Security
Procedures**

Definitions

Accounting: Individuals have a right to receive an accounting of Disclosures of Protected Health Information made by Dunlap (or its Business Associates) in the six years prior to the date on which the Accounting is requested, except for Disclosures made to carry out Treatment, Payment and Health Care Operations, unless the Disclosure was made by electronic medical record, in which case the individual may request an Accounting of all Disclosures, including those for Treatment, Payment and Health Care Operations, during the three years prior to the date on which the Accounting is requested unless Disclosures are restricted by law. An Accounting is not necessary if the Disclosure was made to the individual about his or her own Protected Health Information.

Authorization: Signed document permitting Dunlap to Use or Disclose Protected Health Information (PHI) for purposes other than Treatment, Payment, and Health Care Operations.

Business Associate (B.A.): Vendor or contractor that, in performing a Covered Function for Dunlap, accesses, Uses or Discloses Protected Health Information (*e.g.* accountants, attorneys, consultants). Business Associates are directly subject to HIPAA's Privacy and Security Rules to the same extent as Covered Entities.

B. A. Agreement: Written contract or exhibit to service agreement describing how a Business Associate performs Covered Functions for Dunlap and includes means by which the Business Associate will safeguard Privacy, mitigate damage, notify individuals of Breach, and otherwise comply with HIPAA's Privacy and Security Rules.

Breach: Breach means the unauthorized acquisition, access, Use or Disclosure of unsecured Protected Health Information, which compromises the Privacy or Security of Protected Health Information by posing a significant risk of financial, reputational or other harm to individuals. Breach does not include the unintentional acquisition, access or use of Protected Health Information by a workforce member or Business Associate if the access were made in good faith and within the scope of authority and does not result in further unauthorized Use or Disclosure. Dunlap has a duty to inform affected individuals when a Breach occurs. It also must notify the Secretary of the Department of Health and Human Services and, if the Breach involves more than 500 residents, it must notify the media.

Covered Entity: Health Care Provider, Health Plan, or Health Care Clearinghouse that transmits Protected Health Information electronically. Dunlap, physicians, other health care practitioners, and providers are Covered Entities, as are group health insurers.

Covered Function: Service involving the Use or Disclosure of PHI by a Business Associate for a Covered Entity.

Designated Record Set: Medical records, claims and billing records created or kept by Dunlap in hard copy or electronic format.

Disclosure: Releasing, transferring Protected Health Information, or giving a third party access to Protected Health Information.

Fundraising: Dunlap may contact patients or other persons for Fundraising, which is a Health Care Operation and not Marketing, but Dunlap must in a clear and conspicuous manner notify the recipient of Fundraising information of the opportunity to opt out of receiving further Fundraising communications. When an individual elects not to receive further Fundraising communication, that election operates as a revocation of Authorization.

Health Care Operations: Activities including, but not limited to, Fundraising, quality improvement, case management, credentialing, privileging, focused or ongoing professional practice evaluation, accreditation, root cause analysis, risk management, practitioner evaluations, insurance, contracting, audits, legal defense, legal and accounting services, compliance, business and strategic planning, and administration.

Health Care Provider: Dunlap, other hospitals, physicians, other health care practitioners or providers of health care services and items.

Incidental Disclosure: Disclosure of Protected Health Information despite reasonable safeguards (*e.g.* when a third party overhears an appropriate conversation between Health Care Practitioners involving PHI for Treatment in a clinical setting). An Incidental Disclosure is not considered a HIPAA Violation or Breach.

Marketing: Targeted and direct communication that is not a Health Care Operation, entailing the unauthorized Use and Disclosure of Protected Health Information to encourage recipients to purchase or use a product or service. Dunlap may contact existing or former patients about health care services, including case management, that may benefit them, which is not considered Marketing, so long as Dunlap offers persons the opportunity to opt out of further contacts.

Minimum Necessary Standard: A Covered Entity must limit the access, Use or Disclosure of PHI to the minimum necessary to accomplish the purpose for which Protected Health Information is being requested, Used or Disclosed. Job descriptions may describe Minimum Necessary accessibility.

Notice of Privacy Practices (NPP): Written notice given to patients describing Dunlap's Use and Disclosures of PHI, how Dunlap safeguards Privacy and Security, informing patients of their HIPAA Privacy rights, including the rights to review and amend their medical records, request restrictions, have an accounting, and make a complaint.

Notification: Dunlap, following the discovery of a Breach of Unsecured Protected Health Information, must give written Notification to each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Dunlap to have been, accessed, acquired, used or disclosed as a result of Breach. Dunlap also must give Notification to the Secretary of the Department of Health and Human Services and, if the Breach involves more than 500 residents, Dunlap must give written Notification to the media.

Payment: Compensation or reimbursement for Treatment, (*e.g.* billing, claims management, and collection).

Personal Representative: Designated person who may sign an Authorization for the Use or Disclosure of Protected Health Information on behalf of a patient who lacks capacity because of age or mental infirmity, or who is deceased, (*e.g.* guardian, next of kind, parent, spouse, adult child, brother or sister, executor, attorney, holder of DPOA-HC).

Privacy & Security Coordinator (aka Privacy Officer): Dunlap's Privacy & Security Coordinator is the chief compliance officer overseeing Use and Disclosure of Protected Health Information and reasonably assuring the security of PHI, according to HIPAA's Privacy and Security Rules.

Protected Health Information (PHI): Individually identifiable information (oral or written) about a patient's past, present or future physical or mental condition, Treatment for that condition, and Payment for Treatment, including medical records (paper and EHR) as well as radiological studies, computer drives and networks, audiotapes, photographs and videotapes, created, received transmitted, and maintained by Dunlap.

Qualified Protective Order: with respect to Protected Health Information requested means a "stipulation by the parties to the litigation" that:

- (A) Prohibits the parties from using or disclosing the Protected Health Information for any purpose other than the Pending Litigation or proceeding for which such information was requested; and
- (B) Requires the return to the covered entity or destruction of the Protected Health Information (including all copies) at the end of the Pending Litigation or proceeding.

Request to Restrict Disclosure: An individual may request that Dunlap not Disclose certain Protected Health Information, which Dunlap must honor if the Disclosure is to a Health Plan for purposes of carrying out Payment or Health Care Operations and is not for purposes of carrying out Treatment, and the Protected Health Information pertains solely to a Health Care item or services for which the Health Care Provider has been paid out of pocket in full.

Training: Dunlap has an ongoing obligation to provide continuing education and Training to members of its Workforce regarding Dunlap's obligations under HIPAA, as periodically amended, including information about Dunlap's policies and procedures with respect to Protected Health Information. Training also includes Dunlap's providing a process for individuals to make complaints about actual or suspected HIPAA Violations or Breaches and to make suggestions about improving the policies and procedures without the fear of retaliation. Dunlap may impose appropriate sanctions against members of the Workforce who fail to comply with the privacy policies and procedures.

Treatment: Provision, coordination, or management of a patient's health care and related services by Dunlap and one or more Health Care Providers.

Unsecured Protected Health Information: Unsecured Protected Health Information means Protected Health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary (*e.g.* encryption).

Use: Sharing and providing access to Protected Health Information within Dunlap for Treatment, Payment, and Health Care Operations.

Violation: The unauthorized Use or Disclosure of Protected Health Information.

Workforce: Dunlap's Workforce includes employees, volunteers, trainees, temporary workers, contract workers through agencies and other persons whose conduct in the performance of work for Dunlap is under Dunlap's direct control. Workforce does not ordinarily include Business Associates.

Introduction

HIPAA's Privacy and Security Rules apply to the Use and Disclosure of PHI by Covered Entities and their Business Associates. Dunlap is committed to complying with HIPAA's Privacy and Security Rules. It will use reasonable and appropriate safeguards (including training, job descriptions, and physical and technical safeguards), consistent with its capabilities, to assure that PHI and patient privacy rights are protected and secure.

Members of Dunlap's Workforce, who are in a position to access, Use or Disclose PHI, should ask themselves two basic questions:

- Who is requesting or receiving this PHI?
- What is the purpose for this requested access, Use or Disclosure of PHI?

Generally, PHI may be Used or Disclosed without a signed Authorization if the purpose of the Use or Disclosure involves Treatment, Payment for Treatment, or Dunlap's Health Care Operations. PHI, for example, may be shared, subject to the Minimum Necessary Standard, among members of Dunlap's clinical Workforce involved in taking care of the patient. It may be shared with members of the Medical and Allied Practitioner staffs who are involved in taking care of the patient. It may be Disclosed, subject to the Minimum Necessary Standard, to outside Health Care Providers, including other hospitals, nursing facilities, physicians and other health care providers, who are involved in actual or proposed Treatment of the patient.

Employees, other members of Dunlap's Workforce, Health Care Providers, and others may not access, Use or Disclose PHI, if they are not involved (by job description) in the Treatment of the patient or otherwise involved for Payment or Health Care Operations purposes, unless the patient or patient's Personal Representative has signed an Authorization. No Dunlap employee or member of the Workforce (including spouses) may access a patient's PHI because of curiosity or other unauthorized purpose.

Business Associate (B.A.)

Before Dunlap gives a B.A. vendor access to PHI to perform a Covered Function, the vendor must sign a B.A. Agreement or B.A. Addendum to the Service Agreement that contains the elements in the exemplar attached to these Procedures.

Dunlap does not need to enter into B.A. Agreements with physicians and other health care practitioners, with whom it has a professional services agreement, or with members of Dunlap's workforce.

Dunlap, as necessary, will amend Business Associate Agreements it has with Business Associates that it entered into before 2010, to assure that Business Associates comply with the Privacy and Security requirements applicable to Business Associates to the same extent as Covered Entities, including the requirements for mitigating damages and Notice, and to assure that the Business Associate Agreement indemnifies Dunlap from any claim or penalty arising from any allegation of Violation or Breach by the Business Associate.

Vendors should sign Dunlap's standard B.A. Agreement. Dunlap may sign a vendor's B.A. Agreement if it is substantially similar to Dunlap's standard B.A. Agreement, complies with HIPAA's Privacy and Security Rule requirements that now apply directly to Business Associates, if the Business Associate indemnifies Dunlap for any penalty or claim arising out of a Breach by the Business Associate, and the vendor's Business Associate Agreement does not require Dunlap to indemnify the B.A.

Dunlap must keep all B.A. Agreements on file.

Notice of Privacy Practices (NPP)

Dunlap will post its NPP in a place(s) conspicuous to patients.

New Patients:

- Give a NPP to all new patients (or Personal Representative) at registration or before they receive initial Treatment, unless the patient is unable to sign because of an emergency.
- Have patient sign an acknowledgment of receiving NPP, which will be kept in the patient's record.
- Document reasons for not having a signed acknowledgment if patient refuses or is unable to sign.

Established Patients:

- Check if patient previously received a NPP.
- If patient previously received an NPP, there is no need to give patient another NPP.
- If patient did not previously receive an NPP, give patient a NPP.
- Have patient sign an acknowledgment of receipt and put into patient's record.
- Document attempt to give patient an NPP, if patient refuses or is unable to sign.

Amended Notice of Privacy Practices

Dunlap will amend its Notice of Privacy Practices to conform with amendments as a result of the American Recovery and Reinvestment Act of 2009, and the regulations issued periodically by the Department of Health and Human Services.

Dunlap will give its amended Notice of Privacy Practices to new patients. It will post its amended Notice of Privacy Practices on its website and will further post in conspicuous areas where Notices of Privacy Practices are issued instructions on how patients may request an amended Notice of Privacy Practices.

Directory

Dunlap will inform patients (Personal Representatives) that PHI will be used to create a directory.

Patients may object entirely to being listed in the directory, or they may restrict Disclosure to certain persons whom they identify by name or category.

If the patient objects to being listed in the directory, then Dunlap cannot voluntarily Disclose or confirm any information about the patient, including whether the person is a patient.

If the patient (Personal Representative) does not object, then Dunlap may Disclose the following information in the directory to family, clergy, friends, and others who ask about the patient by name:

- Patient's name
- Location (room)
- Patient's general condition or status
- Patient's religious affiliation

If the patient does not have an opportunity to object to being listed in the directory, because of emergency circumstances, then Dunlap may Use or Disclose PHI listed in the directory if Disclosure is:

- Consistent with the patient's prior preference or practice
- In the patient's best interest, as Dunlap reasonably determines by exercising reasonable discretion.

Dunlap will give the patient (Personal Representative) the opportunity to object when it becomes practical to do so.

Use and Disclosure of PHI for Treatment, Payment and Health Care Operations

Dunlap may Use or Disclose PHI, subject to the Minimum Necessary Standard, to:

- Provide Treatment to patients (inpatient or outpatient).
- Share medical information with other Health Care Providers involved in the patient's Treatment, including physicians on Dunlap's Medical Staff, as well as physicians and health care providers and facilities outside of Dunlap that are involved with the patient's Treatment .
- Obtain Payment or Reimbursement for Treatment to patients. Dunlap does not need an Authorization to share PHI with the patient's health plan, insurer, commercial or governmental third-party payer (including Medicare, Medicaid, and other Federal health care program), HMO and third-party payer.
- Conduct Healthcare Operations.

Reasonable Safeguards

Dunlap will use reasonable safeguards, physical and technical safeguards, including encryption where practicable, consistent with its size and capability, to protect the confidentiality and proper Use and Disclosure of PHI and to minimize the risk of Breach, Violation and Incidental Disclosure.

Safeguards include HIPAA Privacy education and training; job duties and descriptions specifying need (if any) to access PHI; as well as physical and technical safeguards.

Conversations with Patients

Employees should use reasonable efforts when talking to patients about their PHI to protect privacy and prevent those conversations from being overheard by third parties who are not involved in the patient's Treatment.

Reasonable steps, as circumstances warrant, include a reasonable distance away from others, speaking in low volume, or moving the conversation someplace else where it is less likely to be overheard.

Conversations between Employees or with Other Health Care Providers

Employees should use reasonable steps, as circumstances warrant, when discussing patient PHI among themselves or with physicians or other Health Care Providers, protect a patient's privacy, such as lowering the volume of voices or moving the conversation to another location where it is less likely to be overheard.

Medical Records

Employees should use reasonable safeguards in safeguarding PHI that appears in a patient's medical record. Employees, for example, should not leave open records on unattended desks or in areas where members of the public can see them.

Filing cabinets

Only employees with authorized access to the filing cabinets should be allowed to obtain or replace materials in the cabinets.

Fax Machines

Fax machines should be kept in locations where documents containing PHI cannot be viewed by persons who are not involved in the patient's Treatment or who do not have a legitimate access to the transmitted PHI.

Telephones

Reasonable steps should be taken during telephone conversations (land lines and cell phones) regarding patient PHI, such as using private areas, closing doors, or speaking with low volume matters.

Computers

Reasonable steps should be taken to limit access to PHI at employee computer work stations, including prudent use of passwords, screen savers and other technical safeguards.

Laptops must be used solely for authorized Hospital purposes.

Email that contains Protected Health Information will be encrypted, as appropriate and practical.

Breach and Notification

Breach means the unauthorized acquisition, access, use, or disclosure of Protected Health Information, which compromises the security or privacy of such information by posing a significant risk of financial, reputational or other harm to the individual.

Breach excludes: (1) any unintentional acquisition, access or use of Protected Health Information by a Workforce member or person acting under the authority of a Covered Entity or Business Associate if the acquisition, access or use was made in good faith and within the scope of authority and does not result in further use; or (2) Disclosure in an unauthorized manner, or any inadvertent disclosure by a person who is authorized to access Protected Health Information at a Covered Entity or Business Associate to another person authorized to access Protected Health Information at the same Covered Entity or Business Associate, and the information received as a result of such disclosure is not further Used or Disclosed; or

(3) a Disclosure of Protected Health Information where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

Unsecured Protected Health Information means Protected Health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary (*e.g.* encryption).

Notification to individuals:

Following the discovery of a Breach of Unsecured Protected Health Information, Dunlap must notify each individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of Breach.

A Breach shall be treated as Discovered by Dunlap as of the first day on which such Breach is known to Dunlap, or by exercising reasonable diligence would have been known to Dunlap.

Unless notification were to impede a police investigation, Dunlap must notify individuals without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach.

Notification Elements to Individuals:

The Notification must be written in plain language and include:

- Brief description of what happened, including date of Breach and date of discovery, if known.
- Description of types of Unsecured Protected Health Information that were involved in the Breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved.
- Any steps individuals should take to protect themselves from potential harm resulting from Breach.
- Brief description of what Dunlap is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches.
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, e-mail address, web site or postal address.

The written Notice should be sent by first-class mail to the last known address of the individual or to email.

If the individual is deceased, the Notice should be sent to the personal representative.

If the address is insufficient or out of date, the Notice may be posted in print or broadcast media.

Dunlap may contact an individual by telephone in urgent situations in which possible misuse is imminent.

Notification to Media

If Breach of Unsecured Protected Health Information involves more than 500 residents of a State or jurisdiction, Dunlap, following discovery of the Breach, must notify prominent media outlets serving the State or jurisdiction, without unreasonable delay, but in no case later than 60 calendar days after discovery of the Breach.

Notification to the Secretary of DHHS

Following the discovery of a Breach of Unsecured Protected Health Information, Dunlap must notify the Secretary of DHHS.

- If the Breach involves 500 or more individuals, Dunlap will provide notification contemporaneously with the Notice to the individuals.
- If the Breach involves less than 500 individuals, a Dunlap must maintain a log or other documentation of the Breaches and not later than 60 days after the end of each calendar year provide the Notification to the Secretary of DHHS during the preceding calendar year.
- Dunlap's Privacy Officer will maintain the log and will be responsible for notifying, or arranging for proper notification, consistent with the regulations.

Employee and Workforce Access to PHI

Dunlap permits only those employees and members of the Workforce who need access to PHI (subject to the Minimum Necessary Standard) for Treatment purpose and to carry out their authorized job duties.

Because job responsibilities vary between employees, some employees and members of the Workforce may have greater access to PHI, while other employees and Workforce members may have very limited access.

Employees and Workforce members who provide direct patient Treatment, such as physicians and nurses assigned to the patient, may access PHI to perform their job duties. Other employees, such as billing personnel, have limited access to PHI, as defined by their job description.

Dunlap will determine employee levels of access to PHI, which will be established by job description or policy.

Employees and members of its Workforce (including spouses) are not permitted to access, Use or Disclose PHI of patients for any unauthorized purpose, including curiosity or malice.

Improper access, Use or Disclosure of PHI for unauthorized purposes, depending on the frequency or severity, will result in education and/or disciplinary action, including suspension or immediate termination.

Minimum Necessary

Dunlap will make reasonable efforts to Use or Disclose only that amount of PHI that is minimally necessary to accomplish the purpose for which PHI was requested or needed.

The Minimum Necessary Standard does not apply to:

- Disclosures made to the Secretary of DHHS to determine compliance with the Privacy Rule.
- Disclosures required by Federal or Ohio law.

Dunlap will identify employees who need access to PHI to perform their job duties.

Employees will be informed about the level of access to PHI appropriate to the job during employee orientation.

Employees with access to PHI will:

- Use only PHI necessary to accomplish the specific task.
- Not browse through a patient's record unless the particular task requires.
- Not share PHI with co-employees or staff members who do not need it to perform their job duties.

Minimum Necessary: Disclosures to Requests

- Authorizations requesting Disclosure of PHI will be reviewed by the Manager of HIM (or his/her designee) on a case-by-case basis.
- Disclose only that PHI that addresses the request (identified by record, admission, date, problem, *etc.*) stated in the Authorization.
- Seek clarification from the patient or Personal Representative before Disclosing (releasing records), if questions exist.

Disclosure of PHI to Family Members or Personal Representatives

If the patient is present and has capacity:

- Ask the patient permission to Disclose PHI to family members, Personal Representatives, relatives, close personal friends or other persons involved in the patient's Treatment or Payment.
- If the patient agrees or does not object, Disclosure may be made.

If patient is not present, lacks capacity, and in emergency situations:

- PHI may be Disclosed if, in the exercise of professional judgment, it is determined that Disclosure is in the best interests of the patient and it is directly relevant to those involved in the patient's Treatment and well-being.

Disclosure of a Minor's Protected Health Information

Dunlap generally may Disclose a minor's PHI to the minor's parents, including both the mother and father in a divorce situation (regardless of who is the custodial parent, unless there is a court order prohibiting Disclosure), without an Authorization.

Dunlap also may Disclose a minor's PHI to the minor's guardian.

Dunlap may deny a request by a parent or guardian to access or receive the minor's PHI if the decision to deny is made by a licensed health care provider, who in the exercise of professional judgment, determines that Disclosure would not be in the minor's best interest.

Dunlap will honor an emancipated or "mature" (over the age of 14) minor's request to restrict Disclosure of PHI if:

- The minor lawfully can make his or her own health care decisions.
- The minor's parents or guardian previously agreed to a confidential arrangement between the physician and the minor.
- Ohio law does not permit parents or guardian to access the PHI without the minor's Authorization.
- Testing for sexually transmitted diseases, including HIV.
- Obtaining an abortion with approval by the juvenile court.
- Treatment for a condition related to drug or alcohol abuse.
- Treatment related to outpatient mental health care.

An emancipated minor is a person who is less than 18 years old, but who does not live with parents or guardian, is self-supporting, is a member of the military, is married, or is pregnant.

Disclosure of Protected Health Information by Authorization

A patient (Personal Representative) must sign a written Authorization before Dunlap may Disclose PHI for purposes not related to Treatment, Payment, or Health Care Operations.

Purposes not related to Treatment, Payment, or Health Care Operations for which an Authorization is required include, but are not limited to:

- Inquiries from employers
- Inquiries from schools
- Inquiries from life insurance companies or other non-health plan insurers
- Subpoenas and other litigation requests
- Marketing
- Research

The patient also must sign an Authorization before Dunlap may Disclose Psychotherapy Notes.

It is preferable to use Dunlap's standard Authorization. Dunlap may accept other Authorization forms that comply with HIPAA's requirements, which include the requirement of being written in "plain English" and contain the following elements:

- Patient's name
- Description of the PHI to be released.
- Name of the entity or person receiving the Disclosed PHI.
- Description of purpose for the requested Use or Disclosure of PHI.
- Expiration date or event triggering expiration of the Authorization.
- Statement that PHI Disclosed to a third-party may no longer be covered by HIPAA and may be re-disclosed.
- Statement that treatment cannot be conditioned on signing an Authorization.
- Statement of patient rights, including right to revoke the Authorization in writing.
- Patient signature and date.

Authorizations may be delivered in person, by mail, by fax, and by scanned e-mail. Photocopies may be accepted, unless there is reasonable suspicion that the Authorization is fraudulent or invalid.

The Manager of HIM (or his/her designee) should:

- Review the Authorization to assure it contains all required elements. Reject any defective Authorization.
- If the Authorization is missing any required element, do not Disclose any PHI. Contact the patient or Personal Representative.

- Request documentation from the Personal Representative to assure that the Personal Representative has the authority to act on behalf of the patient to Authorize Disclosure of PHI.

A guardian must produce letters of appointment; an executor must produce an entry from the Probate Court; an attorney-in-fact must produce the durable power of attorney for health care decisions.

Occasionally, a deceased patient's "estate" is not probated. There is no executor or administrator. Under those circumstances, Dunlap may Disclose the deceased patient's PHI if the surviving spouse or other person claiming authority to act on behalf of the deceased patient signs a statement of authority and agrees to indemnify Dunlap against any claim for wrongful Disclosure, based on reasonable reliance.

- Dunlap may Disclose only the PHI needed to meet the patient's request as stated in the Authorization and for the purpose stated, according to the Minimum Necessary Standard.
- The Authorization will be maintained with the patient's medical records.

Patient's Right to Revoke an Authorization

A patient may revoke an Authorization in writing, which must be signed and dated.

- When a patient requests Dunlap to revoke an Authorization, document the request, and inform the patient that the request must be in writing and that it will be effective, except to the extent Dunlap already Disclosed PHI in reliance on the Authorization.
- The signed revocation may be sent by facsimile.
- Attach the completed, signed and dated revocation to the Authorization in the patient's file.

If a patient revokes the Authorization, Dunlap must comply with the patient's request.

Mandatory Disclosures and Reporting

Dunlap will disclose PHI without an Authorization if Federal or Ohio law requires.

Questions whether a patient's PHI may be disclosed without an Authorization for mandatory reporting purposes, should be directed to the Privacy & Security Coordinator. Mandatory reporting includes:

- Public health activities: Disease reports required by Ohio law, vital statistics such as birth and death records, reports of child abuse and neglect, for public health surveillance and investigations, reports required by the FDA, reports required by OSHA, and by public health authorities.
- Abuse, neglect or domestic violence: Reports to law enforcement authorities, social service agencies, or protective services agencies required by Ohio law.
- Health oversight activities: Audits, surveys, investigations, inspections, licensure, and disciplinary actions necessary for the appropriate oversight of health care systems, government benefit programs, and health care providers subject to certain government regulations.
- Law enforcement: At the request of a law enforcement official, for reporting certain types of wounds (*i.e.* gunshots, stabbings), or responding to court-ordered warrants, grand jury subpoenas, subpoenas or summonses ordered by a judicial officer, or identification/location of persons.
- Decedents: Disclosures to medical examiners, coroners or funeral directors to identify a deceased person, determine causes of death, or to carry out funeral-related duties.
- Organ donation: Disclosures for cadaver organ, tissue and eye procurement, banking and transplantation.
- Preventing a serious threat to health or safety to a person or the public.

- Specialized government functions: Military and veterans' activities, homeland security, national security and intelligence, medical suitability determinations required by the U.S. Secretary of State, correctional institutions and custodial activities.
- Workers' compensation benefits.

Judicial and Administrative Procedures

Dunlap will Disclose PHI in response to a subpoena or discovery request issued in connection with a civil or administrative proceeding, if there is a signed Authorization, a court order, or a Qualified Protective Order, or if the subpoena requires the custodian of medical records to appear personally at the trial, hearing, grand jury, or administrative proceeding.

The Manager of HIM (or his/her designee) will receive and review all subpoenas and discovery requests.

If the subpoena or discovery request instructs Dunlap to Disclose PHI by sending it to an attorney or for discovery purposes, Dunlap will not Disclose PHI unless:

- There is a valid Authorization.
- A signed court order instructs Dunlap to Disclose PHI by producing medical records described in the subpoena.
- Dunlap receives a written statement from the person requesting the PHI with documentation that the parties have agreed to a Qualified Protective Order, or the person requesting the PHI has made a good faith attempt to provide written notice to the patient and no objections to disclosure have been filed.

Section 154.512(c)(1)(v) of HIPAA's Privacy Rule defines a Qualified Protective Order with respect to Protected Health Information requested, to mean a "stipulation by the parties to the litigation" that:

- (A) Prohibits the parties from using or disclosing the Protected Health Information for any purpose other than the Pending Litigation or proceeding for which such information was requested; and
- (B) Requires the return to the covered entity or destruction of the Protected Health Information (including all copies) at the end of the Pending Litigation or proceeding.

The subpoena, Authorization, order or Qualified Protective Order must be kept with the patient's medical record.

Disclosure of PHI in response to a subpoena or order is subject to the Minimum Necessary Standard.

Criminal Proceedings and Law Enforcement

Dunlap may Disclose PHI to comply with a court order, court-ordered warrant, subpoena or summons issued by a judicial officer in a criminal proceeding or a grand jury subpoena if Disclosure is limited to the relevant requirements of the request according to the Minimum Necessary Standard.

The Manager of HIM (or his/her designee) will receive and review the document.

A copy of the request (*i.e.* court order, court-ordered warrant, etc.) must be kept with the patient's medical record.

Exemption for Red Cross and Armed Forces

Dunlap may Disclose PHI, without an Authorization, to the Red Cross and the Armed Forces to assist it in notifying the patient's family member of the patient's location, general condition or death.

Waiver of HIPAA Requirements in an Emergency or Disaster

If the President declares an emergency or disaster, and the Secretary of DHHS declares a public health emergency, the Secretary may waive the obligation of Dunlap to comply with any or all of the following Privacy requirements:

- The requirement to obtain the patient's agreement to speak to family members or friends involved in the patient's care.
- The requirement to honor a request to opt out of the facility directory.
- The requirement to distribute a Notice of Privacy Practices.
- The patient's right to request privacy restrictions.
- The patient's right to request confidential communications.

The waiver period only applies if Dunlap is in the emergency area for the emergency period and for up to 72 hours until Dunlap implements its disaster protocol.

Serious Threat to Health or Safety

Dunlap may disclose a patient's PHI if necessary for law enforcement authorities to identify or apprehend a person if:

- The patient admitted participation in a violent crime that is reasonably believed to have caused serious physical harm to another person.
- The patient has expressed an intent to harm an identified person and has the present means to carry out the threat or to do harm.
- If, based upon all circumstances, it appears that the patient has escaped from a correctional institution or from lawful custody.

Any Disclosure to avert a serious threat to health or safety must be made in good faith and based upon actual knowledge or reliance on a credible representation by a person with apparent knowledge or authority.

It is advisable to consult the Privacy Officer or legal counsel.

Contacting Patients

Dunlap will use reasonable safeguards when contacting patients by telephone or leaving messages on answering machines.

Check whether the patient has requested that communication be accomplished by alternative means or at an alternative location, or if the patient has restricted the Use or Disclosure of PHI.

- If the call is answered, ask to speak with the patient. If the patient is not available, call back.
- If the call is answered by an answering machine or voice mail, leave a brief message requesting the patient to call the number and extension.

Patient Request for Communication of PHI to an Alternative Location or by an Alternative Means

A patient or patient's Personal Representative may request Dunlap to communicate with him or her at an alternative location or by alternate means. This right allows a patient to direct how and where confidential communications made by Dunlap and concerning PHI are mailed, faxed, emailed or telephoned.

Requests for communicating with the patient at an alternative location or by an alternative means must be in writing.

- The request must be reviewed to determine whether it can be reasonably accommodated.
- If Dunlap can reasonably accommodate the patient's request, it should confirm with the patient the alternative location or alternative means.
- The request and reasonable accommodation must be kept with the patient's contact information.
- If Dunlap cannot reasonably accommodate the patient's request, it must notify the patient, explaining the reason for denying the request and suggesting, if practical, an alternative.

Patient Request to Restrict Disclosure of PHI

An adult patient (Personal Representative), emancipated minor or mature minor may request that Dunlap restrict the Use and Disclosure of PHI. By exercising this right, a patient may request that Dunlap restrict the Use or Disclosure of PHI related to:

- Treatment, payment or health care operations
- Disclosures to persons involved in the patient's care
- Disclosures to notify persons, such as family members, personal representatives, or others responsible for the patient, about Protected Health Information directly relevant to the patient's care or payment for care
- Disclosures to persons when the patient is or is not present
- Disclosures for disaster relief purposes

If Dunlap agrees to a restriction as requested by a patient, Dunlap must abide by the restriction, unless the restriction prevents the provision of emergency care to the patient.

Dunlap must honor the request by a patient or patient's Personal Representative to restrict Disclosure if the restriction is to a Health Plan for purposes of carrying out Payment or Health Care Operations and is not for purposes of carrying out Treatment, and the Protected Health Information pertains solely to a Health Care item or services for which the Health Care Provider has been paid out of pocket in full.

Dunlap is not required to agree to a patient's request to restrict the Use and Disclosure of PHI for Treatment purposes, and Dunlap, absent special circumstances, should not restrict Disclosure of PHI for Treatment purposes.

A patient may not restrict PHI from being Used or Disclosed for:

- Requests by the Secretary of DHHS to investigate or determine compliance with the HIPAA Privacy Rule.
- A facility directory to track patient locations.
- Emergency Treatment.
- Disclosures that do not require an Authorization, such as Disclosure of PHI to public health authorities for reporting a communicable disease.

A patient may terminate the agreed upon restriction, either in writing or verbally. Termination is effective only with respect to PHI created or received after Dunlap is informed by the patient of the decision to terminate the restriction.

Dunlap may terminate the agreed-upon restriction, after notifying the patient of its intent to terminate the restriction and giving the patient the opportunity to agree or object.

The patient must submit a written request to restrict Use or Disclosure of PHI.

The Manager of HIM (or his/her designee), or the Privacy Officer, as applicable, should promptly review the medical record to determine whether the information that the patient wishes to restrict is allowable under the Privacy Rule or whether the information to be restricted will hinder or interfere with the patient's Treatment or Payment for Treatment.

If the request is granted, the Manager of HIM (or his/her designee) will document the restriction in a conspicuous manner near the restricted PHI.

If the request is denied, to inform the patient in writing of the reasons.

A patient may request orally or in writing that Dunlap end the restriction.

Patient Request to Inspect and Copy Protected Health Information

A patient generally may inspect and copy his or her medical records (PHI) in a Designated Record Set.

A "Designated Record Set" means the group of medical and billing records about the patient that Dunlap created, received and maintains.

Dunlap may deny a patient's request (and that denial is not reviewable) to inspect and copy records that include:

- Psychotherapy notes.
- Information compiled in the reasonable anticipation of, or use in, a civil, criminal or administrative proceeding.
- Records protected under Clinical Laboratory Improvement Amendments (CLIA).
- Records subject to the Federal Privacy Act.
- Records that are not part of a Designated Record Set. Quality improvement, peer review, and incident reports are not part of the Designated Record Set and are not available for review and copying.
- Records obtained from someone other than a health care provider under a promise of confidentiality.

Dunlap may deny a patient's request (and that denial is reviewable) to inspect and copy records that include:

- A reasonable determination by a health care provider that access is reasonably likely to endanger the life or physical safety of the patient or another person.
- PHI contains references to another person, and the health care provider determines that access is reasonably likely to cause substantial harm to such other person.
- The request for access is made by the patient's personal representative, and the health care provider determines that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

The patient must make the request to inspect or copy in writing.

Requests should be processed (granted or denied) within 30 days from the date of receipt.

The Manager of HIM (or his/her designee) will review the medical record to determine what information and records are part of a Designated Record Set, whether psychotherapy notes exist, and whether any other information is privileged and not available for inspection.

If the request is granted, the Manager of HIM (or his/her designee) will contact the patient making the request, by mail or by telephone, to arrange for: (a) an appointment for the patient to inspect the records; or (b) the mailing of the requested records (at an address specified by the patient—check for any requests for an alternative address); or (c) the mailing of a summary of PHI *in lieu* of production of the records themselves.

If the patient requests that medical records be copied and sent, have the patient complete an Authorization.

Dunlap may charge the requesting patient copying costs, including the cost of supplies and labor, up to the maximum amount permitted by Ohio law (Revised Code Section 3701.741). Dunlap also may charge for the preparation of the summary, if the patient requests a summary *in lieu* of production of the records. Dunlap may charge for postage if the requested materials are mailed.

If the patient makes an appointment to inspect PHI in the Designated Record Set, allow the patient to inspect the records in a location that reasonably assures privacy.

If the person requesting to inspect the record is the patient's personal representative, photocopy that person's driver's license or identification card. If the person claims to be the patient's "attorney-in-fact" under a Durable Power of Attorney for Healthcare Decisions, or the patient's Guardian or Executor, request a copy of the authorizing document (request in advance before the person comes to Dunlap).

It is not necessary for staff to be present while the patient inspects the record. However, confidential documents, computer access, and PHI regarding other patients must not be accessible to the patient. The patient also must be instructed that he or she cannot remove any original record or make any changes to the record. If the patient wants to “amend” the record, the patient must sign the Request for Amendment form.

If, following inspection, the patient requests a copy of the record, have the patient sign an Authorization, and inform the patient that the copied chart (or requested portions) will be available in 14 days, and inform the patient of any copying charges.

If Dunlap denies the request by the patient to inspect and copy records, send a written denial that specifies in plain language the basis of the denial and any review rights the patient may have.

- If access denial is based on Reviewable Grounds, then inform the patient of the right to have the denial reviewed by another licensed health professional, appointed by Dunlap, to act as a reviewing official. The reviewing official must not have participated in the original decision to deny.
- Promptly provide the reviewing official with the review request.
- The reviewing official must determine within a reasonable time (no more than 30 days) if to deny access.
- The reviewing official's determination must be promptly transmitted in a written notice to the patient.

Request to Amend or Correct Protected Health Information in the Patient's Record

A patient or Personal Representative may request to amend incorrect, inaccurate or incomplete PHI contained in a Designated Record Set .

Dunlap may deny the request if the PHI:

- Was not created by Dunlap, unless the patient provides a reasonable basis to believe that the original source of the incorrect, inaccurate or incomplete PHI no longer is available.
- Is not part of a Designated Record Set.
- Is accurate and complete.
- Consists of psychotherapy notes.
- Is compiled in reasonable anticipation of, or for use in, a criminal, civil or administrative proceeding.
- Is subject to requirements of the Clinical Laboratory Improvement Amendments (CLIA).
- Was obtained from someone other than a health care provider under a promise of confidentiality.

The patient must make a written request to amend PHI in a Designated Records Set.

The request must be kept with the patient's medical record.

The Manager of HIM (or his/her designee) will review the request and the medical record to determine:

- What records are included in a Designated Record Set.
- Whether psychotherapy notes exist.
- Whether any record is privileged or not available for the patient to amend.

Requests should be processed (granted or denied) within 60 days from the date of receiving the request.

- If requests cannot be processed within 60 days, Dunlap may extend the time to reply for an additional 30 days by providing the patient with a written statement describing both the reasons for the delay and the date in which it anticipates responding. Only one extension of time is permitted by the Privacy Rule.

If the request to amend is granted, the Manager of HIM (or his/her designee) will:

- Inform the patient that the request was granted and to ask the patient to identify the relevant persons who should receive the amended information.
- Make the appropriate amendment to the patient's PHI. Do not change, obliterate or delete the existing information in the patient's record. Append the amendment to the record or provide a link to the location of the amendment in the record.
- Make reasonable efforts to inform and provide the amended information, within a reasonable time, to (1) parties identified by the patient, and (2) parties, such as Business Associates, whom Dunlap knows may have the patient's PHI that is the subject of the amendment and who could rely on the un-amended, incorrect or incomplete information to the detriment of the patient.

If the request is denied, the Manager of HIM (or his/her designee) must timely inform the patient of the denial in a writing that:

- Informs the patient in plain language that he or she may send a written statement of disagreement to Dunlap and that this written statement will be included with all future disclosures of Protected Health Information that is subject to the requested amendment.
- Describes how the patient may submit a complaint using Dunlap's Complaint Resolution Process including the name, title and telephone number of the Privacy & Security Coordinator, or to the Secretary of DHHS.

After receiving the patient's written statement of disagreement, Dunlap may prepare a written rebuttal, which will be placed with the patient's medical record. A copy of the rebuttal must be mailed to the patient.

Dunlap must identify the PHI in the Designated Record Set subject to the disputed amendment and attach the patient's request, Dunlap's denial letter, patient's written statement of disagreement, and Dunlap's rebuttal.

For all future Disclosures of the patient's PHI subject to amendment:

- If the patient submitted a written statement of disagreement, it must be included with all subsequent disclosures of PHI, or, in the alternative, Dunlap may include an accurate summary of the information.
- If the patient did not submit a written statement of disagreement, Dunlap must include the patient's request to amend and denial letter, or in the alternative, Dunlap may include an accurate summary of the information.
- If a transaction of PHI does not allow the transmission of the additional information concerning the request to amend, Dunlap should separately transmit the additional information to the recipient of the transaction.

Dunlap must document the names and titles of the persons responsible for receiving and processing requests to amend and retain the documentation for at least six years. If Dunlap receives an amendment of a patient's PHI from another Health Care Provider or entity, Dunlap must amend the patient's PHI as contained in a Designated Record Set at Dunlap, according to the steps described above.

Request for an Accounting

A patient may request an Accounting of Disclosures by Dunlap of his or her PHI during the previous six years.

An Accounting of Disclosures includes:

- The date PHI was Disclosed.
- The name and address of the entity or person receiving PHI, if known.
- A brief description of PHI Disclosed;
- A brief statement of the purpose of the Disclosure that reasonably informs the patient of the basis for the Disclosure, or a copy of the written request to Disclose PHI as required by the Secretary of DHHS, or a copy of the request for PHI for which an Authorization is not required (see Mandatory Disclosures and Reporting Policy);
- The frequency, periodicity or number of Disclosures made to the person or entity.
- The date of the last Disclosure during the accounting period if multiple disclosures were made to a single person or entity.

An Accounting does not include Disclosures Dunlap made:

- Before April 14, 2003.
- For Treatment, Payment and Health Care Operations, except as provided below.
- Directly to the patient or Personal Representative.
- Incident to Use or Disclosure permitted by the Privacy Rule.
- In response to an Authorization.
- To include the directory.
- To persons involved in the patient's care.
- To correctional institutions or law enforcement officials.

If a health oversight agency or law enforcement official provides Dunlap with a written or oral statement notifying it that an Accounting of Disclosures will reasonably impede the agency's or official's activities, Dunlap must not inform the patient about these Disclosures.

If a Disclosure of Protected Health Information is made by electronic medical record, the individual may request an Accounting of all Disclosures, including those for Treatment, Payment and Health Care Operations during the three years prior to the date on which the Accounting is requested, subject to the exceptions stated above.

The patient must give Dunlap a written request for an Accounting, which Dunlap must keep with the patient's medical record.

The request will be forwarded to the Privacy Officer, who will review whether the requested information may be Disclosed to the patient in an Accounting.

Dunlap has 60 days to respond to the patient's request. If an Accounting cannot be made within 60 days, an additional 30 days may be available if the patient is provided with a written statement describing the reason for the delay and the date by which Dunlap will give Accounting. Only one extension is permitted by the Privacy Rule.

If the request for an accounting is granted, the Accounting will include the Disclosures described in the Policy.

If this is the first request for an Accounting by the patient in a 12-month period, Dunlap may not charge the patient for preparing the Accounting for the Disclosure.

If the patient submits a subsequent request for an Accounting in the same 12-month period, Dunlap may charge the patient reasonable costs for preparing the Accounting, unless Disclosure was made electronically, in which case Dunlap may not charge.

If the patient's request for an Accounting is denied, a written notice should be faxed, mailed or emailed to the patient explaining the reason for the denial.

Complaint Resolution Procedure

Dunlap will inform patients of a Complaint Resolution Process of their right to complain about Dunlap's privacy policies and procedures. Patients may also file a complaint if they believe their privacy rights have been violated. Patient complaints will go to the Privacy & Security Coordinator for prompt investigation and disposition. Patients also must be notified of their ability to complain directly to the Office for Civil Rights of the Department of Health and Human Services or to the Ohio Attorney General.

A patient may make a complaint orally or in writing. A patient may make a complaint anonymously.

Assure the patient, if known, that his or her Complaint will be immediately investigated. Inform the patient that Dunlap will use its best efforts to respond to the Complaint as soon as possible, but not later than 30 days.

The Privacy & Security Coordinator will record all Complaints in the appropriate log book, indicating:

- The date the Complaint was received and the nature of the Complaint.
- The date when violation allegedly occurred.
- Name of person(s) who allegedly violated the patient's privacy right.
- Description of the investigation.
- Any actions taken.
- Correspondence or feedback provided to the patient.

The Privacy & Security Coordinator will analyze the Complaint by interviewing the patient or person, employees and staff members, or by other methods of investigation as necessary and appropriate.

If the complaint is substantiated, Dunlap will implement appropriate and reasonable remedial actions to resolve the Complaint. This may entail revising Dunlap's HIPAA policies and procedures, job responsibilities, additional training, or taking disciplinary action.

If the patient's Complaint is not reasonable or is unsubstantiated, a letter should be sent to the patient summarizing the results of the investigation and an explanation of findings.

The patient must be informed, whether the Complaint is validated or not, that he or she may submit a complaint to the Secretary, Department of Health and Human Services. Provide the Secretary's address in any letter sent to the patient.

The following statement should be included in follow-up letters to patients making Complaints:

Because we understand your concerns about the privacy and confidentiality of medical and health information, it is our policy not to retaliate against any patient making a complaint directly to us or to the Secretary, Department of Health and Human Services.

Patient Complaints should not be kept with the patient's medical record.

The patient's Complaint, along with any follow-up letters and investigation documentation, should be kept in a separate HIPAA-compliance file, or the complaint log book, maintained by the Privacy & Security Coordinator.

HIPAA Education and Training

Dunlap will train the workforce about HIPAA Privacy and Security, as periodically amended by statute or regulations, including information about Dunlap's policies and procedures with respect to Protected Health Information. Training also includes Dunlap's providing a process for individuals to make complaints about actual or suspected HIPAA Violations or Breaches and to make suggestions about improving the policies and procedures without the fear of retaliation. Dunlap may impose appropriate sanctions against members of the Workforce who fail to comply with the privacy policies and procedures.

Dunlap will train new employees about HIPAA's Privacy Rule and how it affects their job responsibilities, including informing them of their level of access, Use and Disclosure of PHI, during employee orientation.

Dunlap may require employees to undergo additional training and education if there are changes in the law or if problems are identified.

Employees will sign an Employee Statement of Confidentiality

By signing the Employee Statement of Confidentiality, an employee acknowledges that every employee shares the duty to protect a patient's confidentiality, and that the employee agrees to:

- Properly Use and Disclose PHI according to these Policies and Procedures.
- Only access PHI needed to carry out job responsibilities.
- Take reasonable steps to safeguard and protect the privacy and confidentiality of patient PHI.
- Report concerns about suspected violations and privacy breaches.
- Maintain and protect the privacy and confidentiality of patient PHI during and after employment at Dunlap.

The signed Employee Statement of Confidentiality will be placed in the employee's personnel file.

Duty to Report Privacy Violations or Breaches

Employees have a duty to report HIPAA Privacy Violations or Breaches, as well as concerns about the privacy or confidentiality of Protected Health Information, to the Privacy & Security Coordinator.

A report may be made in writing or verbally.

Employees may identify themselves or may report privacy breaches or concerns anonymously.

All reports will be kept confidential.

There will be no retaliation against any person who reports a suspected Breach or Violation in good faith.

An employee who fails to report a Breach or Violation may, depending on circumstances, be subject to further education or disciplinary action.

Privacy & Security Coordinator (aka Privacy Officer)

Dunlap will appoint a qualified person to be the Privacy & Security Coordinator, who will oversee HIPAA policies and procedures for safeguarding Privacy and Security.

The Privacy & Security Coordinator will work closely with technical personnel on Security matters.

The Privacy & Security Coordinator will oversee HIPAA compliance, including education and training requirements, responding to questions whether to Use or Disclose PHI, and investigating complaints by patients, employees, or others.

The Privacy & Security Coordinator will be the primary liaison on any investigation or communication with the Office for Civil Rights of DHHS.

The Privacy & Security Coordinator will report to Dunlap's Compliance Committee and will recommend amendments to HIPAA-related documents and practices, as appropriate.

Investigation

Dunlap will cooperate with the Office for Civil Rights of DHHS and Ohio Attorney General in investigations of alleged HIPAA Violations or Breaches. Investigations are complaint-driven. Investigations may lead to civil, criminal or administrative actions, which could lead to monetary penalties.

Dunlap may receive notice of an investigation by mail, by telephone or in person.

If a letter, subpoena or telephone call is received and is related to an investigation, immediately forward it to a Privacy & Security Coordinator.

Do not destroy, alter or hide patient files or documents.

Answer questions honestly, but do not volunteer any information not requested.

Cooperate with those persons conducting the investigation.

Questions or concerns about the investigation should be directed to the Privacy & Security Coordinator, who may involve legal counsel.

Amendments

The Privacy & Security Coordinator, on his/her own volition at least every 3 years (or if there is a material amendment in the regulations), at the request of an employee, or at the recommendation by legal counsel, will review Dunlap's Privacy and Security Policies and other HIPAA-related documents and will make recommendations to the Compliance Committee and Dunlap's administration.