PROCEDURE: **HIPAA: Marketing and PHI**

Authority: **45 CFR 164.514(e)(1); 42 CFR 418(c)(5); 418.104(c); 418.116**

Purpose: **When Hospice of North Idaho's marketing communications involve the use or disclosure of an individual's protected health information to encourage recipients to use or purchase products or services, an authorization from the individual is obtained as required by Federal regulations.**

Cross Reference:

Effective Date:

Revised: **4.1.11 ; 9.3.13** ; 1.7.16

Definition:

Marketing: *A communication about a product or service that encourages recipients of the communication to purchase the product or service.*

Financial remuneration: *Direct or indirect payment from or on behalf of a third party whose product or service is being marketed.*

PROCEDURE:

1. Hospice of North Idaho evaluates its marketing communications to determine if protected health information is involved.
2. For marketing communications that involve the use or disclosure of protected health information for which the hospice is receiving financial remuneration from a third party, an authorization from the patient is obtained unless the marketing communication takes place during a face to face encounter or involves products or services of nominal value.
3. Marketing communications do not include the following communications provided no financial remuneration is received for making the communications:
    - about the participating providers and health plans in a network, the services offered by the providers, or the benefits covered by a health plan;
    - about the individual's treatment; or
    - involve case management or care coordination of the individual, or directions or recommendations for alternative therapies or treatments, to the extent these activities do not fall within the definition of treatment.

PROCEDURE: **HIPAA: Breach Notification Requirements**

Authority: 42 CFR 164.402- 164.414

Purpose: Hospice of North Idaho follows Federal and State requirements related to the notification of individuals when a breach of unsecured protected health information is discovered.

Cross Reference:

Effective Date: **4.1.11**
Revised Date: **9.19.13** ; 1.7.16

Definitions

Breach **-** *means the acquisition, access, use or disclosure of protected health information in a manner not permitted by the Privacy Rule, which compromises the security or privacy of the protected health information.*

Unsecured protected health information *– protected health information that is not rendered unusable, unreadable, or indecipherable by encryption or destruction.*

Affected individual – *the person whose PHI was breached.*

PROCEDURE:

1. All incidents related to a suspected or actual breach of unsecured protected health information are reported to the Privacy Officer as soon as discovered.
2. An immediate investigation is conducted and the *Breach Risk Assessment* is completed and its findings are documented in the *Breach Risk Assessment Summary*.
3. Based on the findings of the investigation and the *Breach Risk Assessment*, a determination is made regarding whether or not there is a probability that the protected health information has been compromised and therefore constitutes a reportable breach.
4. If the incident does not constitute a reportable breach, the Privacy Officer retains the documented findings of the *Breach Risk Assessment* and the *Breach Risk Assessment Summary* for six years from the date the incident occurred.
5. If a reportable breach has occurred, relevant information is gathered for the breach notification letter to be sent to affected individuals as soon as possible but no later than sixty (60) calendar days from the date of the discovery of the breach.
6. The written breach notification letter is sent by first class mail to the last known address of the affected individual(s).
7. If the affected individual is deceased, the written notification letter may be sent to the individual's next of kin or personal representative if their contact information is available.

8. If the affected individual is deceased and contact information for next of kin or the personal representative is inaccurate or unavailable, no further notification requirements are required although the breach will be included in the agency's accounting of reportable breaches to the government.
9. If Hospice of North Idaho is unable to reach more than 10 of the affected individuals, the agency will post a conspicuous notification on its Web site for 90days and /or notify the media in the location(s) where the affected individuals are believed to reside.
10. If a breach affects more than 500 individuals in a specific State or jurisdiction, prominent media outlets will be contacted within 60 calendar days of discovery of the breach, and a prominent notice will be placed on the agency's Web site in addition to the individual notification of affected individuals.
11. If more than 500 individuals are affected by a breach, Hospice of North Idaho will notify HHS within 60 calendar days of discovery of the breach following the instructions posted on its Web site.
12. For each breach that occurs within a calendar year that affects less than 500 individuals, Hospice of North Idaho will maintain documentation of all information related to the breach and its investigation and provide an accounting of all such breaches to HHS within 60 days following the end of the calendar year. This accounting is provided in accordance with instructions posted on HHS' Web site.
13. All documentation related to all breaches discovered by the agency or any of its business associates is maintained for six years from the date of discovery of the breach.

PROCEDURE: **HIPAA: Business Associates**

Authority: 45 CFR 160.103; 45 CFR 164.502; 45 CFR 164.504(e)(i); 45 CFR 164.308 (b)(10; 45 CFR 164.410(a)(b)(c); HITECH Act, Sect. 13401 (a)(b) and 13402(b); 42 CFR 418.52(c)(5); 418.104(c)

Purpose: A contract or contract addendum with a business associate is signed before the business associate is allowed to create, receive, maintain, or transmit protected health information on behalf of Hospice of North Idaho (HONI).

Cross Reference:

Effective Date: **9.23.13** ; 1.7.16

Definition: *A business associate is any person or entity that creates, receives, maintains or transmits protected health information on behalf of the hospice or to perform a service for the hospice. A business associate may not use or disclose protected health information in a manner not permitted by HIPAA regulations.*

PROCEDURE:

1. Existing and new relationships with non-members of the hospice's workforce are reviewed to determine if a business associate relationship exists.
2. Business associates that use, disclose, create, receive, maintain, or transmit protected health information on behalf of HONI are required to sign a written contract that assures that the business associate is aware of its responsibilities with regard to protected health information and compliance with HIPAA regulations.
3. HONI relies on the business associate to determine the type and the minimum necessary amount of protected health information necessary for their purposes.
4. Business associates are aware of their obligations and the obligations of their subcontractors to comply with the applicable standards of the HIPAA Privacy Rule, the HIPAA Security Rule and the Breach Notification Rule.
5. Business associates are required to make a report to the hospice of any privacy violation, security incident or breach of unsecured protected health information within two business days of business associate's discovery of the violation, incident or breach.
6. The Privacy Official will monitor the return or destruction of the protected health information used, created or obtained by the business associate upon termination of the contract.
7. Known violations of a material term of the contract or contract addendum may result in termination of the business associate relationship.

BUSINESS ASSOCIATE AGREEMENT

HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement is effective on _____, and is entered into between covered entity Hospice of North Idaho, Inc. ("CE") and _____ ("Associate") dated _____.

RECITALS

A. CE does not wish to disclose information ("Information") to Associate that is considered Protected Health Information ("PHI").

B. CE and Associate intend to protect the privacy and provide for the security of PHI disclosed to Associate pursuant to this Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated hereunder by the U.S. Department of Health and Human Services ("the HIPAA Regulations") and other applicable laws.

C. The purpose of this form is to satisfy certain standards and requirements of HIPAA and the HIPAA Regulations, including, but not limited to, Title 45, parts 160 and 164 of the Code of Federal Regulations ("CFR"), as the same may be amended from time to time.

In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

1. DEFINITIONS.

1.1 "**Business Associate"** shall have the meaning provided under the HIPAA Regulations, including, but not limited to, title 45 CFR Section 160.103.

2.2 **"Covered Entity"** shall have the meaning provided under HIPAA and the HIPAA Regulations, including, but not limited to, title 45 CFR Section 160.103.

3.3 **"Protected Health Information"** or **"PHI"** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to 45 CFR Section 164.501.

2. ASSOCIATE OBLIGATIONS.

2.1. Permitted Uses and Disclosures. Associate **may not use** and/or disclose PHI that it may come in contact with in performing its contracted duties and responsibilities for CE.

Nondisclosure. Associate shall not use or further disclose CE's PHI otherwise than as permitted or required by this Agreement or as required by law

- **Business Associate's Operations.** Associate may come in contact with PHI only to the extent necessary for Business Associate's proper management and administration or to carry out Business Associate's contracted

duties and responsibilities. Business Associate may disclose such PHI as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities only if the disclosure is required by law

.

2.2 Safeguards. Associate shall use appropriate safeguards to prevent the use or disclosure of CE's PHI other than as provided for by this Agreement. Associate shall make every effort not to access or view PHI.

2.3 Reporting of Disclosures. Associate shall report to CE any use or disclosure of CE's PHI of which Associate becomes aware which falls outside the uses and disclosures contemplated under this Agreement.

2.4 Associate's Agents. Associate shall ensure that its employees, agents, and subcontractors will agree to the same restrictions, conditions and obligations to protect PHI as are imposed on Associate by the Agreement. When agents and subcontractor receive CE's PHI the Associate shall document such disclosures of PHI and information related to such disclosures as would be required for HONI to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with title 45, Part 164, Subpart E, Section 164.528 of the CFR.

2.5 Internal Practices. Associate shall make it's internal practices to document any disclosure of PHI received from, or created and/or maintained on behalf of, CE available to the Secretary of the U.S. Department of Health and Human Services ("DHHS") for purposes of determining Associate's compliance with HIPAA and the HIPAA Regulations.

2.6 Breach.

2.6.1 Notification. During the term of this Agreement, Associate shall notify CE within twenty-four (24) hours of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. The notification shall at least include the following: (a) identify the nature of the unauthorized use or disclosure; (b) identify the PHI used or disclosed; (c) identify who made the unauthorized use or received the unauthorized disclosure; (d) identify what Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; (e) identify what corrective action Associate has taken or shall take to prevent future similar unauthorized use or disclosure; and (f) provide such other information, including a written report, as reasonably requested by HONI compliance officer.

2.6.2 Mitigation. Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of PHI by Associate in violation of the requirements of the Agreement.

2.6.3 Termination for Cause. Upon HONI knowledge of a material breach by Associate, HONI shall:

- Provide an opportunity for Associate to cure the breach or end the violation and terminate if Associate does not cure the breach or end the violation within the time specified by HONI.
- Immediately terminate the agreement if Associate has breached a material term of the agreement and cure is not possible.
- If neither termination nor cure is feasible, HONI shall report the violation to the Secretary of the Department of Health and Human Services.

2.6.4 Judicial or Administrative Proceedings. Either party may terminate this Agreement, effective immediately, if (i) the other party is named as a defendant in a criminal proceeding for a violation of HIPAA or (ii) a finding or stipulation

that the other party has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

2.7 Effect of Termination. Upon termination of this Agreement for any reason, Associate shall return any PHI that Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, as determined by CE, Associate shall continue to extend the protections of this Agreement to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

3. CE OBLIGATIONS.

CE shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Associate pursuant to this Agreement, in accordance with the standards and requirements of HIPAA and the HIPAA Regulations, until such PHI is received by Associate. Any specifications defining the point of receipt of CE's PHI by Associate shall be set forth in Exhibit A.

4. AUDITS, INSPECTION & ENFORCEMENT.

From time to time, upon reasonable notice and determination by CE that Associate has breached this Agreement, CE may inspect the facilities, systems, books and records of Associate to monitor compliance with this Agreement. Associate shall promptly remedy any violation of any term of this Agreement and shall certify such remedy in writing to CE.

5. INDEMNIFICAITON.

Each party will indemnify, hold harmless and defend the other party to this Agreement from and against any and all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in connection with: (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the party of the party under this Agreement; and (ii) any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with the party's performance under this Agreement.

6. DISCLAIMER.

CE makes no warranty or representation that compliance by Associate with this Agreement, HIPAA or the HIPAA Regulations will be adequate or satisfactory for Associate's own purposes or that any information in Associate's possession or control, or transmitted or received by Associate, is or will be secure from unauthorized use or disclosure. Associate is solely responsible for all decisions made by Associate regarding the safeguarding of PHI.

8. AMENDMENT.

1. Automatic Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to electronic date security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. Upon the effective date of any amendment to the regulations promulgated by DHHS with respect to PHI, the Agreement shall automatically amend such that the obligations imposed on Associate as a Business Associated remain in compliance with such regulations. CE may terminate this Agreement upon thirty (30) days written notice in the event (i) Associate does not enter

into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA Regulations.

9. ASSISTANCE IN LITIGATION AND/OR ADMINISTRATIVE PROCEEDINGS.

Associate shall make itself, and any subcontractors, employees or agents assisting Associate in the performance of its obligations under this Agreement, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon any claimed violation of HIPAA, the HIPAA Regulations or other laws relating to security and privacy, except where Associate or its subcontractor, employee or agent is a named adverse party.

10. NO THIRD PARTY BENEFICIARIES.

Nothing express or implied in this Agreement is intended to confer, nor shall confer, any rights, remedies, obligations, or liabilities whatsoever upon any person other than CE, Associate and their respective successors or assigns.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Agreement Effective Date.

Hospice of North Idaho <COVERED IDENTITY>	<ASSOCIATE>
_____	_____
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

PROCEDURE: **HIPAA: Complaint Resolution**

Authority: 42 CFR 418.52(b)(1)(iii); 45 CFR 164.530(d)(1); 45 CFR 164.530(g)(1); 42 CFR 164.414(a)

Purpose: Hospice of North Idaho has a complaint resolution process that is implemented whenever a complaint is received.

Cross Reference:

Effective Date: **4.1.11**
Revised Date: **9.19.13**; 1.7.16

PROCEDURE:

1. Hospice paitents/caregivers are informed of their right to lodge complaints without fear of discrimination, reprisal or interruption of care, treatment, and service.
2. Hospice patients/caregivers are informed of their right to lodge complaints about whatever concerns they might have, including but not limited to: care or lack of care received; any violations or concerns related to the agency's privacy practices including any actual or potential breaches of the patient's health information or violation of any other patient rights.
3. Hospice of North Idaho's admission materials include a description of the complaint resolution process and the contact information for the agency and the State hotline (including hours of operation) that may be used to lodge a complaint.
4. Complaints/concerns brought to the direct attention of any agency employee or volunteer are addressed immediately whenever possible and brought to the attention of the Clinical Director.
5. All complaints are documented in a complaint log by the Clinical Director no more than five (5) business days from the date of the complaint was first received.
6. A documented investigation is conducted by appropriate personnel of all written or verbal complaints received by the agency.
7. To resolve complaints, a minimum of three (3) attempts are made to contact the person filing the complaint by telephone. If telephone contact is unsuccessful, a letter is sent. Each contact, attempted contact, or action taken to resolve the issue is documented with the original complaint.
8. Complaints or concerns expressed on a written survey are reviewed initially by the Clinical Director and then forwarded to the agency Administrator if appropriate. Follow-up is initiated whenever possible to resolve complaints or concerns.
9. Corrective action is implemented, as appropriate, in response to substantiated complaints.
10. Complaints are tracked and regularly reviewed to identify patterns or trends and performance improvement opportunities.

11. HONI employees and volunteers receive training regarding the agency's complaint resolution process.
12. Complaints that involve a breach of PHI receive immediate follow-up in accordance with HONI's breach notification policies and procedures.

PROCEDURE: **HIPAA: Fundraising and Protected Health Information**

Authority: 45 CFR 164.514(f)(1)(2); HITECH Act, SEC. 13406(b); 42 CFR 418.52(c)(5); 418.104(c)

Purpose: Hospice of North Idaho complies with the requirements of the HIPAA Privacy Rule with regard to uses and disclosures of protected health information for targeted fundraising communications.

Cross Reference:

Effective Date: **4.1.11**
Revised: **9.19.13** ; 1.7.16

Definition:
Fundraising communication: ***When a hospice, its institutionally related foundation or business associate uses or discloses protected health information for targeting communications for the purpose of raising funds for the hospice, the communication may be made in writing, by direct mail, via email or by a verbal communication.***

PROCEDURE:

1. The agency's *Notice of Privacy Practices* includes a statement that the individual's protected health information may be used or disclosed for targeted fundraising communications. In addition, the Notice of Privacy Practices states that individuals have the right to opt-out of receiving fundraising communications from the hospice.
2. Only the following protected health information is used in targeting fundraising communications:
    a. Demographic information, including name, contact information, age, date of birth, and gender;
    b. Dates of health care provided to an individual; department of service information;
    c. Treating physician;
    d. Outcome information; and
    e. Health insurance status.
3. Only the minimum amount of PHI necessary to accomplish the intended purpose of the fundraising communication is used or disclosed.
4. All targeted fundraising communications include a clear and conspicuous opportunity to elect not to receive any further fundraising communication and how to do so.
5. Hospice of North Idaho provides an opt-out mechanisms in all fundraising communications that do not cause the recipient to incur an undue burden or more than a nominal cost.

6. Hospice of North Idaho maintains a database of all individuals who have elected to opt-out of receiving future fundraising communications and treats that individual's election as a revocation of authorization.
7. Hospice of North Idaho ensures that no further fundraising communications are sent to individuals who have exercised their right to opt-out.
8. Individuals who have opted out of receiving further fundraising communications are provided with a method to opt back in at a future date.
9. The hospice does not condition treatment or payment on the individual's choice with regard to receiving fundraising communications
10. Hospice of North Idaho only uses specific information about the treatment of a patient (e.g. for videos, brochures, and testimonials in fundraising solicitations) if it obtains written authorization to do so.

PROCEDURE: **HIPAA: Patient Requests for Access to Protected Health Information**

Authority: 45 CFR 164.524(a); 42 CFR 418.52(c)(5); 418.104(c)

Purpose: Patients or their personal representatives have the right to request to inspect or obtain a copy of their health information.

Cross Reference:

Effective Date:
Revised Date: **9.19.13** ; 1.7.16

PROCEDURE:

1. Hospice of North Idaho (HONI) requires and informs individuals that requests for access to personal health information must be made in writing.
2. When a request for access to health information is received, it will be acted upon within thirty (30) days. An extension of no more than thirty (30) days is allowed if the hospice provides the individual with a written statement that specifies the reason(s) for the delay and the date by which the individual may expect to receive access to the health information for inspection or to obtain a copy.
3. The hospice maintains the designated record sets in which the health information that may be subject to requests for access is contained for a period of six years from the date it was created or was last in effect, whichever is later.
4. The hospice maintains the titles of the persons/offices responsible for receiving and processing requests for access for a period of six years.

When a request for access is denied

1. The individual is given a statement written in plain language that explains the reasons for the denial decision and the individual's right to a review of the decision with an explanation of how to exercise this right.
2. To the extent possible, the hospice will grant access to other health information for which there were no grounds to deny access.
3. The hospice will designate a licensed health care professional, not involved in the original denial decision, to serve as a reviewing official and reevaluate the request for access if the individual requests such a review.

When a request for access is accepted (in whole or in part)

1. The individual is notified of the decision and may choose to inspect the health information, copy it, or both, in the form or format requested.
2. If the individual agrees, the hospice may provide a summary of the requested health information for an additional charge.
3. Access to the protected health information is granted in the form and format requested by the individual. If the protected health information is not readily

producible in the form and format requested, a readable hardcopy form or other format as agreed upon will be provided.

4. If the requested PHI is maintained electronically in one or more designated records sets, the protected health information must be provided to the individual in the electronic form and format requested by the individual. If the requested form and format is not readily producible, the hospice must offer an alternative readable electronic format. If the individual does not agree to the alternative format, a hard copy may be provided to fulfill the request for access.
5. The hospice and the individual will arrange a mutually convenient time and place for the individual to inspect and/or obtain a copy of the requested information.
6. The hospice must mail a copy of the requested health information if the individual prefers this method of obtaining a copy.
7. The hospice will transmit the copy of the PHI directly to another person provided that the request to do so is made in writing, signed by the individual and includes clear identification the designated person and where to send the protected health information.

Fees charged by HONI for access to health information

1. The hospice charges a reasonable, cost based fee for copying, labor and supplies (for instance, paper, computers disks, and postage).
2. No fee is charged for retrieving or handling the requested information or for processing the individual's request for access to their health information.
3. The hospice may charge a nominal fee for preparing an explanation or summary of the requested information if the individual is informed of and agrees to a summary of the information and is willing to pay the fee.

PROCEDURE: **HIPAA: Privacy and Security Awareness Training for Staff and Volunteers**

Authority: **45 CFR 164.533(b); 45 CFR 168.308 (b); 45 CFR 164.530(b)(1)(2); 42CFR418.52(c)(5);418.104(c); 42 CFR 164.414(a)**

Purpose: Hospice of North Idaho provides training regarding privacy and security policies, procedures and practices for all current and new employees, including management, and volunteers who have contact with protected health information.

Cross Reference: **Security Training**
Effective Date:
Revised: **4.1.11 ; 9.19.13** ; 1.7.16

PROCEDURE:

1. All new employees, including management, and volunteers with PHI access receive privacy and security training as a component of their orientation to Hospice of North Idaho prior to access of PHI and the information system is authorized.
2. Staff members, including management, and volunteers with access to ePHI receive security training as appropriate to their job responsibilities and whenever there are changes to the hospice's security environment.
3. All staff members of Hospice of North Idaho, including volunteers, receive retraining if privacy or security awareness policies and procedures change and as necessary. These procedures include protection from malicious software, log-in monitoring, password management and reporting privacy or security incidents.
4. Periodic security reminders are provided to all staff, including management, and volunteers with ePHI access, to ensure awareness of security issues and concerns related to PHI.
5. A formal security training program is provided during the orientation program for new staff and volunteers before access to ePHI and the agency's information system is authorized.
6. Emphasis is placed, throughout the trainings, on procedures for identifying and reporting potential or actual privacy or security incidents, including those that involve a breach of protected health information.
7. All privacy and security awareness training provided to staff members and volunteers is documented and maintained in personnel records or by the Privacy and Security Officers for 6 years from the date the training was provided.

PROCEDURE: **HIPAA: Safeguarding Protected Health Information (PHI) Maintained by Clinical Staff Outside the Medical Record**

Authority: **45 CFR 164**

Purpose: Hospice of North Idaho staff is required to safeguard PHI that is outside the medical record to ensure that PHI is not improperly disclosed, discussed, or electronically transmitted.

Cross Reference: **Security Training; Security Framework and Access Management; Password Management; Access Control Integrity**

Effective Date: **07.28.06**
Revised: **01.22.14; 3.2.16**

PROCEDURE:

1. Hospice of North Idaho staff will be oriented in all HIPAA responsibilities, including safeguarding PHI maintained outside the medical record.
2. Specific safeguards to be taken by staff, include but are not limited to the following:
    - Minimum amount of PHI will be carried outside the office.
    - PHI shall not be left visible on unattended desk tops or computer screens.
    - Log out of the computer when not attended.
    - Do not share computer login or password with anyone.
    - Do not keep passwords in a visible place near your computer.
    - Ensure that PHI maintained outside the medical record is protected in all locations.
    - Use a fax cover sheet with confidentiality statement when disclosing PHI via fax.
3. Report violations or potential privacy violations to the Privacy or Security Official.
4. Posting of client/family "Thank You Notes" will be hung upstairs and/or in areas not accessed by visitors.
5. Reasonable safeguards to protect PHI in staff mailboxes will include but are not limited to the following:
    - Mailboxes will be emptied on a regular basis by each staff member.
    - Supervisors will ensure that a peer is responsible to secure PHI for staff members when they are off work for extended periods of time.
    - All PHI for staff will be placed in envelopes in the staff member's mailbox.

PROCEDURE: **HIPAA: Sanctions for Privacy or Security Violations**

Authority: *45 CFR 164.5530(e)* *42 CFR 164.414(a)*
45 CFR 164.308(i)(c);164.530(e)(1)
42 CFR 418.52(c)(5);418.104(c)

Purpose: Hospice of North Idaho applies appropriate sanctions against any staff or volunteer member who fails to comply with the privacy and security policies and procedures and practices of the organization.

Cross Reference: HONI Sanction Policy; Administrative Sanctions Guidelines
Effective Date:
Revised: **4.1.11 ; 9.19.13**; 1.7.16

PROCEDURE:

1. Hospice of North Idaho staff are provided with training and retraining as necessary to ensure they understand the organization's privacy and security practices and its expectations that staff and volunteers will adhere to them.
2. All staff and volunteers are required to adhere to the privacy and security policies and procedures and practices at HONI. All staff members and volunteers will be made aware that sanctions will be applied for non-compliance of privacy and security procedures and practices.
3. Sanctions for privacy and security violations, including violations of the breach incident reporting requirements, are applied uniformly across all job categories in accordance with HONI's disciplinary action policy and procedure.
4. If a staff member or volunteer commits a privacy or security violation or fails to notify the Privacy Officer of a suspected or actual breach of protected heath information, an immediate investigation will be conducted by the appropriate officer, either Privacy Officer or Security Officer, or their designee, to determine the nature and severity of the violation.
5. All violations will initially be recorded on the HONI Occurrence Report and routed to Privacy or Security Officer for follow-up.
6. The Privacy or Security Official, or their designee, determines the necessary and appropriate sanctions based on the nature of the violation, its severity and whether it was intentional or unintentional.
7 Sanctions may include counseling, verbal warnings, written warnings, probationary periods, termination of access rights to PHI, suspension periods or termination of employment or volunteer status.
8. Any sanctions applied are documented by the appropriate officer, Privacy Officer or Security Officer, and retained for a period of six years from the date the sanctions were applied or last in effect, whichever is later.
9. Sanctions are not applied against any member of Hospice of North Idaho's workforce who engage in whistleblower activities including lodging complaints with any entity regarding violations of Hospice of North Idaho's privacy practice.

PROCEDURE: **HIPAA: Minimum Necessary Disclosure of Protected Health Information**

Authority: 45 CFR 164

Purpose: Hospice of North Idaho employees and business associates disclose the minimum amount of protected health information necessary to achieve the purpose of disclosure.

Cross Reference:

Effective Date: **4.14.03**
Revised Date: **4.1.11; 9.19.13**; 1.7.16

PROCEDURE:

Routine and recurring disclosures of health information:

- HONI has identified disclosures of health information it makes on a routine and recurring basis that are not related to treatment.
- HONI has determined the minimum amount of health information that is needed to achieve the purpose of these requests.

Non-Routine disclosures of health information:

- HONI reviews non-routine requests for disclosures of health information that are not related to treatment on a case-by-case basis unless the patient has authorized the request.
- The request for disclosure is forwarded to the Privacy Official or Compliance Officer to determine if the amount of health information is the minimum necessary to achieve the purpose of the disclosure according to established criteria.
- HONI relies on representation that the information requested is the minimum amount necessary if the request is from a public official, a health care provider, a health plan, a professional providing services to HONI as a business associate, or a researcher (who provides appropriate documentation).
- When necessary or appropriate, the Privacy Official or Compliance Officer will speak with a representative from the entity making the request for clarification and/or modifications.

Disclosures of Entire Medical Records:

- HONI does not disclose an individual's entire medical record in fulfillment of any request not related to treatment for any reason unless a justification for such a disclosure is documented.

PROCEDURE: **HIPAA: Minimum Use Necessary Uses of Protected Health Information**

Authority: 45 CFR 164

Purpose: Hospice of North Idaho employees and volunteers use the minimum amount of protected health information necessary to perform their job functions.

Cross Reference:

Effective Date: **4.14.03**
Revised Date: **4.1.11; 9.19.13** ; 1 7.16

PROCEDURE:

1. HONI has adopted a role-based minimum necessary use of protected health information to identify the employees and volunteers who need access to protected health information according to the categories of uses for treatment, payment or health care operations.
    a. HONI identifies the type and minimum amount of protected health information needed by employees and volunteers to perform their jobs.
    b. HONI determines the circumstances under which employees and volunteers may use protected health information.
    c. Clinical software allows HONI to set up the amount of protected health information by the roe assigned and then can assign additional security to items by individual responsibilities.
    d. A report can be run from clinical software program that shows security assigned by role and by individual.
2. All members of the Interdisciplinary team, student interns and others who provide and coordinate treatment for HONI patients have access to the patient's entire medical record.
3. All employees and volunteers are required to use protected health information in accordance with the determination made by HONI of the minimum amount necessary to effectively perform their jobs.
4. When an employee performs more than one job functions at HONI, the types of protected health information and conditions for access is dependent on the capacity in which the employee is functioning.

Role-Based Minimum Necessary Uses Of Protected Health Information for Treatment Clinical and Family Services		
Position	**Categories/Amount of Protected Health Information**	**Conditions for Access**
Medical Director	Entire Medical Record	Treatment and review
Clinical Director/Nurse Manager	Entire Medical Record	Care and review
Registered Nurses (including case managers, on-call, per diem, triage, etc.)	➢ The entire Medical Record of the patients that a nurse provides direct care to. ➢ PHI of other patient's may be disclosed in aiding other professionals in the care of their patients. ➢ Most nurses are assigned several on-call shifts per month which requires access to entire medical record of all hospice patients.	➢ Care and review ➢ Interdisciplinary Team Meetings
Patient Care Coordinator	Entire Medical Record	Care and review
Hospice Aides (HA)	➢ The entire Medical Record of the patients that a HA provides direct care to. ➢ PHI of other patient's may be disclosed in aiding other professionals in the care of their patients.	➢ Care and review ➢ Interdisciplinary Team Meetings
Director of Social Services	Entire Medical Record	Care and review
Social Workers (SW)	➢ The entire Medical Record of the patients that a SW provides direct care to. ➢ PHI of other patient's may be disclosed in aiding other professionals in the care of their patients. ➢ Social Workers are assigned several on-call shifts per month which requires access to entire medical record of all hospice patients.	➢ Care and review ➢ Interdisciplinary Team Meetings
Bereavement Counselors	➢ The entire Medical Record of a patient when counselor provides direct care to the patient or the patient's family. ➢ PHI of other patient's may be disclosed in aiding other professionals in the care of their patients.	➢ Care and review ➢ Interdisciplinary Team Meetings

Role-Based Minimum Necessary Uses Of Protected Health Information for Treatment Clinical and Family Services		
Caregiving Volunteers	The entire Medical Record of the patients that the volunteer provides direct care to. The Director of Volunteers or the Director of Social Services will approve access to PHI.	Care
Spiritual Care Provider	➢ The entire Medical Record of a patient when Spiritual Care provides direct care to the patient or the patient's family. ➢ PHI of other patient's may be disclosed in aiding other professionals in the care of their patients	➢ Care and review ➢ Interdisciplinary Team Meetings
Other Therapists (i.e. PT, OT, Dietician, Speech)	➢ The entire Medical Record of the patients that the professional provides direct care to. ➢ PHI of other patient's may be disclosed in aiding other professionals in the care of their patients.	➢ Care and review ➢ Interdisciplinary Team Meetings
IT Personnel	➢	➢
Clinical Support Staff	➢	➢
Human Resources	➢	➢
Community Outreach	➢	➢
Marketing	➢	➢

PROCEDURE: **HIPAA: Patient Privacy Rights**

Authority: *45 CFR 164.520; Omnibus Rule*

Purpose: Hospice of North Idaho (HONI) implements policies and procedures to accommodate patient privacy rights as required by and specified by the Privacy Rule of the Administrative Simplification provisions of HIPAA.

Cross Reference: **Client's Rights and Advanced Directive; Notice of Privacy Practices; HIPAA Privacy and Security Awareness Training; Patient Privacy and Marketing**

Effective Date: **1.22.14**

Revised: **4.14.03; 3.11**

PROCEDURE:

Patients cared for by Hospice of North Idaho have the following rights with respect to the privacy of their health information:

- To receive a paper copy of the hospice's *Notice of Privacy Practices*
- To lodge complaints about the hospice's privacy practices
- To request restrictions on the uses and disclosures of health information
- To request to receive confidential communication
- To access their protected health information for inspection and/or copying
- To amend their health care information
- To request an accounting of disclosures of health information
- To opt-out of fundraising
- To receive a notification of a breach

The privacy policies of Hospice of North Idaho detail the requirements for each of these rights and provide the procedures for implementation.

Staff at Hospice of North Idaho is provided with annual training regarding patient rights with respect to their health information.

Information related to patient privacy rights is included in the orientation program for new staff and volunteers.

The hospice's *Notice of Privacy Practices* includes patient privacy rights.

PROCEDURE: **HIPAA: Protected Health Information of Deceased Individuals**

Authority: 45 CFR 164.502(f); 42 CFR 418.52(c)(5); 418.104(c); 418.116 ; Omnibus Rule

Purpose: Hospice of North Idaho protects the health information of deceased hospice patients in the same manner and to the same extent as it did prior to the patient's death.

Cross Reference:

Effective Date:
Revised: **9.19.13** ; 1.7.16

PROCEDURE:

1. Protection of the privacy of a deceased patient's protected health information is provided for fifty (50) years after the patient's death.
2. The hospice may use or disclose the PHI about individuals who have been deceased for more than 50 years for any purpose.
3. A personal representative of the deceased person (someone with legal authority to act on behalf of the deceased person or his or her estate) may exercise the deceased person's rights with respect to protected health information.
4. The identity of the personal representative and his or her authority to act on behalf of the deceased individual is verified according to standard hospice procedures.
5. Hospice may disclose information about a decedent to family members or others involved in the patient's care unless such disclosures would be inconsistent with the prior expressed preferences of the patient.

PROCEDURE: **HIPAA: Privacy and Security Awareness Training for Staff and Volunteers**

Authority: **45 CFR 164.533(b); 45 CFR 168.308 (b); 45 CFR 164.530(b)(1)(2); 42CFR418.52(c)(5);418.104(c); 42 CFR 164.414(a)**

Purpose: Hospice of North Idaho provides training regarding privacy and security policies, procedures and practices for all current and new employees, including management, and volunteers who have contact with protected health information.

Cross Reference: **Security Training**
Effective Date:
Revised: **4.1.11 ; 9.19.13** ; 1.7.16

PROCEDURE:

1. All new employees, including management, and volunteers with PHI access receive privacy and security training as a component of their orientation to Hospice of North Idaho prior to access of PHI and the information system is authorized.
2. Staff members, including management, and volunteers with access to ePHI receive security training as appropriate to their job responsibilities and whenever there are changes to the hospice's security environment.
3. All staff members of Hospice of North Idaho, including volunteers, receive retraining if privacy or security awareness policies and procedures change and as necessary. These procedures include protection from malicious software, log-in monitoring, password management and reporting privacy or security incidents.
4. Periodic security reminders are provided to all staff, including management, and volunteers with ePHI access, to ensure awareness of security issues and concerns related to PHI.
5. A formal security training program is provided during the orientation program for new staff and volunteers before access to ePHI and the agency's information system is authorized.
6. Emphasis is placed, throughout the trainings, on procedures for identifying and reporting potential or actual privacy or security incidents, including those that involve a breach of protected health information.
7. All privacy and security awareness training provided to staff members and volunteers is documented and maintained in personnel records or by the Privacy and Security Officers for 6 years from the date the training was provided.

PROCEDURE: **HIPAA: Requests for Restrictions on the Use or Disclosure of Protected Health Information**

Authority: 45 CFR 164.522(a); HITECH Act, Sect. 13405(a); 42 CFR 418.52(c)(5); 418.104(c)

Purpose: Patients or their representatives have the right to request restrictions on how their protected health information is used and/or disclosed for treatment, payment and health care operations.

Cross Reference:

Effective Date:
Revised Date: **9.19.13**; 1.7.16

PROCEDURE:

1. Patients are informed of their right to request restrictions on the use and disclosure of their protected health information in the agency's Notice of Privacy Practices.
2. All requests by patients for restrictions on the use and disclosure of their health information must be forwarded to the Privacy Official or designee for approval.
3. Hospice employees may not grant or deny a patient's request for restrictions without prior authorization from the Privacy Official or designee.
4. The hospice will agree to a patient's request for restrictions on the use and disclosure of their health information if it is reasonable and in the patient's best interests.
5. The hospice will always agree to a patient's request for restrictions on the use and disclosure of their health information if:
    a. the disclosure is to a health plan for purposes of carrying out healthcare operations or payment (and not for treatment purposes), except as required by law; and
    b. the PHI pertains solely to a healthcare item or service for which the company has been paid in full by the individual, out of pocket.

When a request for restriction(s) is accepted:

1. The patient is informed of any potential consequences of the restriction.
2. A notation is made in writing in the patient's medical record.
3. The hospice will not use or disclose protected health information inconsistent with the agreed restriction, nor will its business associates.
4. The patient is informed that the hospice is not required to comply with the agreed upon restriction(s) in emergency treatment situations.
5. If the agreed upon restriction hampers treatment, the hospice asks the patient to modify or revoke the restriction and gets written agreement to the modification or revocation or documents an oral agreement.

6. The use and/or disclosure of protected health information is consistent with the status of the restriction in effect on the date it is used or disclosed.
7. Written documentation of the agreed to restriction is maintained for six years from the date of its creation or the date when it was last in effect, whichever is later.

A request for restriction(s) may be denied:

1. If the restriction would negatively affect the patient's care;
2. If the restriction is not in the patient's best medical interest;
3. The restriction is for items or services that have been paid in full out of pocket but in fact the payment has not been made despite reasonable efforts to obtain payment; and/or
4. The request is unreasonable and would make the provision of care impossible.

When a request for restriction(s) is denied by HONI:

1. The patient is provided with an explanation of the reasons for the denial.
2. The patient is given the opportunity to discuss his or her privacy concerns if desired.
3. Efforts will be made to assist the patient in modifying the request for restrictions to accommodate their concerns and obtain agreement by HONI.

OCR PRIVACY BRIEF

SUMMARY OF THE HIPAA PRIVACY RULE

HIPAA Compliance Assistance

SUMMARY OF
THE HIPAA PRIVACY RULE

Contents

SUMMARY OF
THE HIPAA PRIVACY RULE

Introduction

The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). [1] The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in notes at the end of this document. To view the entire Rule, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa. In the event of a conflict between this summary and the Rule, the Rule governs.

Links to the OCR Guidance Document are provided throughout this paper. Provisions of the Rule referenced in this summary are cited in endnotes at the end of this document. To review the entire Rule itself, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa.

Statutory & Regulatory Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions.

HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within

	three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.[2] In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.[3] A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E on the OCR website: http://www.hhs.gov/ocr/hipaa.
Who is Covered by the Privacy Rule	The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use the decision tool at: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp. **Health Plans.** Individual and group plans that provide or pay the cost of medical care are covered entities.[4] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,[5] or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance. **Health Care Providers.** Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

	Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. [7] In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.[8] Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.
Business Associates	**Business Associate Defined.** In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.[9] Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity. **Business Associate Contract.** When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.[10] Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule. Covered entities that have an existing written contract or agreement with business associates prior to October 15, 2002, which is not renewed or modified prior to April 14, 2003, are permitted to continue to operate under that contract until they renew the contract or April 14, 2004, whichever is first.[11] Sample business associate contract language is available on the OCR website at: http://www.hhs.gov/ocr/hipaa/contractprov.html. Also see OCR "Business Associate" Guidance.
What Information is Protected	**Protected Health Information.** The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "*protected health information (PHI)*."[12]

	"Individually identifiable health information" is information, including demographic data, that relates to: • the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual, or • the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. **De-Identified Health Information.** There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[15]
General Principle for Uses and Disclosures	**Basic Principle.** A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[16] **Required Disclosures.** A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[17] See OCR "Government Access" Guidance.
Permitted Uses and Disclosures	**Permitted Uses and Disclosures.** A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and

(6) Limited Data Set for the purposes of research, public health or health care operations.[18] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[19] A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See OCR "Treatment, Payment, Health Care Operations" Guidance.

> ***Treatment*** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[20]
>
> ***Payment*** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
>
> ***Health care operations*** are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[22]

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.[23]

Obtaining "consent" (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities.[24] The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

> ***Facility Directories.*** It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility.[25] The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.
>
> ***For Notification and Other Purposes.*** A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care. [26] This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.[27] See OCR "Incidental Uses and Disclosures" Guidance.

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.[28] These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

> ***Required by Law.*** Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by

statute, regulation, or court orders).[29]

Public Health Activities. Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.[30] See OCR "Public Health" Guidance; CDC Public Health and HIPAA Guidance.

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[31]

Health Oversight Activities. Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.[32]

Judicial and Administrative Proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.[33]

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.[34]

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.[35]

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.[36]

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.[37] The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.[38] A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).[39] See OCR "Research" Guidance; NIH Protecting PHI in Research.

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.[40]

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.[41]

	Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.[42] See OCR "Workers' Compensation" Guidance. **(6) Limited Data Set**. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.[43] A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.
Authorized Uses and Disclosures	**Authorization.** A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.[44] A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[45] An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.[46] **Psychotherapy Notes[47].** A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions[48]: • The covered entity who originated the notes may use them for treatment. • A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law. **Marketing.** Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule carves out the following health-related activities from this definition of marketing: • Communications to describe health-related products or services, or payment

	for them, provided by or included in a benefit plan of the covered entity making the communication; • Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan; • Communications for treatment of the individual; and • Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual. Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact. See OCR "Marketing" Guidance.
Limiting Uses and Disclosures to the Minimum Necessary	**Minimum Necessary.** A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.[50] A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. See OCR "Minimum Necessary" Guidance. The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules. **Access and Uses.** For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of

	protected health information to which access is needed, and any conditions under which they need the information to do their jobs. **Disclosures and Requests for Disclosures.** Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures,* that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria. **Reasonable Reliance.** If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.
Notice and Other Individual Rights	**Privacy Practices Notice.** Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans. See OCR "Notice" Guidance. • **Notice Distribution.** A covered health care provider with a *direct treatment relationship* with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows: o Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery); o By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and o In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether *direct treatment providers* or *indirect treatment providers* (such as laboratories) or *health plans* must supply notice to anyone on request.[52] A covered entity must also make its notice electronically available on any web site it maintains for customer service or benefits information.

The covered entities in an *organized health care arrangement* may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.[53] Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

- **Acknowledgement of Notice Receipt.** A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.[54] The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Access. Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's *designated record set*.[55] The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.[56] The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.[57] Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment. The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is

	inaccurate or incomplete.[58] If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.[59] If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity. **Disclosure Accounting.** Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.[60] The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date. The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities. **Restriction Request.** Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.[61] A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[62] **Confidential Communications Requirements.** Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.[63] For example, an individual may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card. Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

Administrative Requirements	HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources. **Privacy Policies and Procedures.** A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64] **Privacy Personnel.** A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.[65] **Workforce Training and Management.** Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).[66] A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68] **Mitigation.** A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.[69] **Data Safeguards.** A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.[70] For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. See OCR "Incidental Uses and Disclosures" Guidance. **Complaints.** A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.[71] The covered entity must explain those procedures in its privacy practices notice.[72] Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS. **Retaliation and Waiver.** A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.[73] A covered entity may not

	require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.[74] **Documentation and Record Retention.** A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[75] **Fully-Insured Group Health Plan Exception.** The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.[76]
Organizational Options	The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections. **Hybrid Entity.** The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity."[77] (The activities that make a person or organization a covered entity are its "covered functions."[78]) To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A covered entity that does not make this designation is subject in its entirety to the Privacy Rule. **Affiliated Covered Entity.** Legally separate covered entities that are affiliated by common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.[79] The designation must be in writing. An affiliated covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions. **Organized Health Care Arrangement.** The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as "organized health care arrangements."[80] Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement's joint health care operations.[81] **Covered Entities With Multiple Covered Functions.** A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.[82] The covered entity may not use or disclose the protected health information of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function.

	Group Health Plan disclosures to Plan Sponsors. A group health plan and the health insurer or HMO offered by the plan may disclose the following protected health information to the "plan sponsor"—the employer, union, or other employee organization that sponsors and maintains the group health plan[83]: • Enrollment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan. • If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. "Summary health information" is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified protected health information). • Protected health information of the group health plan's enrollees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the protected health information. These restrictions must include the representation that the plan sponsor will not use or disclose the protected health information for any employment-related action or decision or in connection with any other benefit plan.
Other Provisions: Personal Representatives and Minors	**Personal Representatives.** The Privacy Rule requires a covered entity to treat a *"personal representative"* the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.[84] A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual. **Special case: Minors.** In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment. See OCR "Personal Representatives" Guidance.

State Law	**Preemption.** In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.[85] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[86] The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits. **Exception Determination.** In addition, preemption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law: • Is necessary to prevent fraud and abuse related to the provision of or payment for health care, • Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation, • Is necessary for State reporting on health care delivery or costs, • Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or • Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
Enforcement and Penalties for Noncompliance	**Compliance.** Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule.[87] The Rule provides processes for persons to file complaints with HHS, describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews. **Civil Money Penalties.** HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.[88] That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

	Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment.[89] The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.
Compliance Dates	**Compliance Schedule.** All covered entities, except "small health plans," must be compliant with the Privacy Rule by April 14, 2003.[90] Small health plans, however, have until April 14, 2004 to comply. **Small Health Plans.** A health plan with annual receipts of not more than $5 million is a small health plan.[91] Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts.[92] See What constitutes a small health plan?
Copies of the Rule & Related Materials	The entire Privacy Rule, as well as guidance and additional materials, may be found on our website, http://www.hhs.gov/ocr/hipaa.

End Notes

[1] Pub. L. 104-191.

[2] 65 FR 82462.

[3] 67 FR 53182.

[4] 45 C.F.R. §§ 160.102, 160.103.

[5] Even if an entity, such as a community health center, does not meet the definition of a health plan, it may, nonetheless, meet the definition of a health care provider, and, if it transmits health information in electronic form in connection with the transactions for which the Secretary of HHS has adopted standards under HIPAA, may still be a covered entity.

[6] 45 C.F.R. §§ 160.102, 160.103; *see* Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). The transaction standards are established by the HIPAA Transactions Rule at 45 C.F.R. Part 162.

[7] 45 C.F.R. § 160.103.

[8] 45 C.F.R. § 164.500(b).

[9] 45 C.F.R. § 160.103.

[10] 45 C.F.R. §§ 164.502(e), 164.504(e).

[11] 45 C.F.R. § 164.532

[12] 45 C.F.R. § 160.103.

[13] 45 C.F.R. § 160.103

[14] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[15] The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the "safe harbor" method of de-identification: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses: (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and ® any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information. 45 C.F.R. § 164.514(b).

[16] 45 C.F.R. § 164.502(a).

[17] 45 C.F.R. § 164.502(a)(2).

[18] 45 C.F.R. § 164.502(a)(1).

[19] 45 C.F.R. § 164.506(c).

[20] 45 C.F.R. § 164.501.

[21] 45 C.F.R. § 164.501.

[22] 45 C.F.R. § 164.501.

[23] 45 C.F.R. § 164.508(a)(2)

[24] 45 C.F.R. § 164.506(b).

[25] 45 C.F.R. § 164.510(a).

[26] 45 C.F.R. § 164.510(b).

[27] 45 C.F.R. §§ 164.502(a)(1)(iii).

[28] *See* 45 C.F.R. § 164.512.

[29] 45 C.F.R. § 164.512(a).

[30] 45 C.F.R. § 164.512(b).

[31] 45 C.F.R. § 164.512(a), (c).

[32] 45 C.F.R. § 164.512(d).

[33] 45 C.F.R. § 164.512(e).

[34] 45 C.F.R. § 164.512(f).

[35] 45 C.F.R. § 164.512(g).

[36] 45 C.F.R. § 164.512(h).

[37] The Privacy Rule defines research as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." 45 C.F.R. § 164.501.

[38] 45 C.F.R. § 164.512(i).

[39] 45 CFR § 164.514(e).

[40] 45 C.F.R. § 164.512(j).

[41] 45 C.F.R. § 164.512(k).

[42] 45 C.F.R. § 164.512(l).

[43] 45 C.F.R. § 164.514(e). A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses: (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any comparable images. 45 C.F.R. § 164.514(e)(2).

[44] 45 C.F.R. § 164.508.

[45] A covered entity may condition the provision of health care solely to generate protected health information for disclosure to a third party on the individual giving authorization to disclose the

information to the third party. For example, a covered entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual's authorization to disclose the results of that examination to the life insurance issuer. A health plan may condition enrollment or benefits eligibility on the individual giving authorization, requested before the individual's enrollment, to obtain protected health information (other than psychotherapy notes) to determine the individual's eligibility or enrollment or for underwriting or risk rating. A covered health care provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual's protected health information for the research. 45 C.F.R. 508(b)(4).

[46] 45 CFR § 164.532.

[47] "Psychotherapy notes" means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the of the individual's medical record. Psychotherapy notes excludes 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 the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R. § 164.501.

[48] 45 C.F.R. § 164.508(a)(2).

[49] 45 C.F.R. §§ 164.501 and 164.508(a)(3).

[50] 45 C.F.R. §§ 164.502(b) and 164.514 (d).

[51] 45 C.F.R. §§ 164.520(a) and (b). A group health plan, or a health insurer or HMO with respect to the group health plan, that intends to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, must state that fact in the notice. Special statements are also required in the notice if a covered entity intends to contact individuals about health-related benefits or services, treatment alternatives, or appointment reminders, or for the covered entity's own fundraising.

[52] 45 C.F.R. § 164.520(c).

[53] 45 C.F.R. § 164.520(d).

[54] 45 C.F.R. § 164.520(c).

[55] 45 C.F.R. § 164.524.

[56] 45 C.F.R. § 164.501.

[57] A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional (who is designated by the covered entity and who did not participate in the original decision to deny), when a licensed health care professional has determined, in the exercise of professional judgment, that: (a) the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (b) the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or (c) the request for access is made by the individual's personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting

to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. § 552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 C.F.R. § 164.524.

[58] 45 C.F.R. § 164.526.

[59] Covered entities may deny an individual's request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 164.526(a)(2).

[60] 45 C.F.R. § 164.528.

[61] 45 C.F.R. § 164.522(a).

[62] 45 C.F.R. § 164.522(a). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

[63] 45 C.F.R. § 164.522(b).

[64] 45 C.F.R. § 164.530(i).

[65] 45 C.F.R. § 164.530(a).

[66] 45 C.F.R. §160.103.

[67] 45 C.F.R. § 164.530(b).

[68] 45 C.F.R. § 164.530(e).

[69] 45 C.F.R. § 164.530(f).

[70] 45 C.F.R. § 164.530(c).

[71] 45 C.F.R. § 164.530(d).

[72] 45 C.F.R. § 164.520(b)(1)(vi).

[73] 45 C.F.R. § 164.530(g).

[74] 45 C.F.R. § 164.530(h).

[75] 45 C.F.R. § 164.530(j).

[76] 45 C.F.R. § 164.530(k).

[77] 45 C.F.R. §§ 164.103, 164.105.

[78] 45 C.F.R. § 164.103.

[79] 45 C.F.R. §164.105. Common ownership exists if an entity possesses an ownership or equity interest of five percent or more in another entity; common control exists if an entity has the direct or indirect power significantly to influence or direct the actions or policies of another entity. 45 C.F.R. §§ 164.103.

[80] The Privacy Rule at 45 C.F.R. § 160.103 identifies five types of organized health care arrangements:

- A clinically-integrated setting where individuals typically receive health care from more than one provider.
- An organized system of health care in which the participating covered entities hold themselves out to the public as part of a joint arrangement and jointly engage in

utilization review, quality assessment and improvement activities, or risk-sharing payment activities.

- A group health plan and the health insurer or HMO that insures the plan's benefits, with respect to protected health information created or received by the insurer or HMO that relates to individuals who are or have been participants or beneficiaries of the group health plan.
- All group health plans maintained by the same plan sponsor.
- All group health plans maintained by the same plan sponsor and all health insurers and HMOs that insure the plans' benefits, with respect to protected health information created or received by the insurers or HMOs that relates to individuals who are or have been participants or beneficiaries in the group health plans.

[81] 45 C.F.R. § 164.506(c)(5).

[82] 45 C.F.R. § 164.504(g).

[83] 45 C.F.R. § 164.504(f).

[84] 45 C.F.R. § 164.502(g).

[85] 45 C.F.R. §160.203.

[86] 45 C.F.R. § 160.202.

[87] 45 C.F.R.§ 160.304

[88] Pub. L. 104-191; 42 U.S.C. §1320d-5.

[89] Pub. L. 104-191; 42 U.S.C. §1320d-6.

[90] 45 C.F.R. § 164.534.

[91] 45 C.F.R. § 160.103.

[92] Fully insured health plans should use the amount of total premiums that they paid for health insurance benefits during the plan's last full fiscal year. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine proxy measures to determine their total annual receipts.

HOSPICE OF NORTH IDAHO

Procedure:	**HIPAA Use and Disclosure Rules**
Authority:	**45 CFR 164.502 - .514**
Purpose:	**Hospice of North Idaho will honor our patient's rights and will follow the federal guidelines in the use and disclosure of their protected health information.**
Cross Reference:	**Notice of Privacy Practice** **Authorization for Psychotherapy Notes** **Valid Authorizations** **Request of an Accounting of Disclosures for PHI** **Minimum Necessary Standard**
Effective Date:	**March 2011**

Procedure:

1. Hospice of North Idaho staff and volunteers will use or disclose patient protected health information per HIPAA and HITECH regulations.
2. The following phi can be released without a signed authorization, for the following purposes:
    - **a.** For treatment or payment purposes or health care operations
        - **i.** Treatment = treating; managing; consulting; referring; etc
        - **ii.** Payment = billing; pre-authorization; collections; consumer reporting agencies; etc.
        - **iii.** Health Care Operations = quality assessment and review activities; review competence, care or performance of staff/volunteers; licensing, accreditation, certification or training; legal or accounting services, auditing, compliance programs; business planning and development; business management and administration; benchmarking.
    - **b.** For disclosures if you give the patient a chance to agree or object
    - **c.** Fits within regulatory exceptions (See Notice of Privacy Practice)
3. HONI staff may disclose relevant information to family or others involved in the care of patient. Information must be limited to the scope of person's involvement. Disclosure may be made in person, over the phone, or in writing.
    - **a.** If patient is present, you may disclose if patient agrees or has chance to object
    - **b.** If patient is present and it is reasonable to infer agreement from circumstance
    - **c.** If patient unable to agree, may disclose if it is determined to be in the best interest of the patient.

4. HONI and Facility staff may disclose limited information (name, location in facility, general condition) from a facility director if:
    a. The patient was given the Notice of Privacy Practice and does not object and
    b. The requestor asks for the person by name.
5. If patient unable to agree or object, HONI staff may use or disclose info for directory if:
    a. The staff member is reasonably sure that the patient has involved the person in the patient's care, and
    b. Determine that, based on staff's professional judgment, the disclosure is in patient's best interests (ex. Allow someone to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of phi)
6. All other exceptions must be logged by the Privacy Official and the records kept for a minimum of six years. Exceptions that would not require an authorization include:
    a. Other laws that require disclosure
    b. Serious threats to health or safety of an individual or the public
    c. Public health activities such as infectious disease, reporting abuse or neglect
    d. Health oversight agencies for audits, investigations etc.
    e. Judicial or Administrative action if have signed order by judge or administrative tribunal or other requests if patient has been given notice and a chance to object
    f. Law enforcement if have court order or other legal document
    g. May release protected information on staff/volunteer to the extent necessary to comply with workers compensation laws
    h. Coroners and funeral directors
    i. Organ donation if patient had requested
    j. Certain research purposes
    k. Military personnel
    l. National security and intelligence purposes
7. Valid authorizations are required psychotherapy notes and all other disclosures (ex. Marketing, some research projects, unless a regulatory exception applies.
8. See Valid Authorizations procedure and Minimum Necessary Standard procedure for more details.