BACKGROUND ........................................................................................................................................ 2

IMPLEMENTATION AND OPERATIONAL CHALLENGES ................................................................... 2

Restrictions .......................................................................................................................................... 2
Determining the Scope of the Designated Record Set ........................................................................ 4
Determining the Scope of the Mental Health DRS ............................................................................ 4
Shadow Records ................................................................................................................................ 5
Operationalizing the Family Members “Safe Harbor” ........................................................................ 5
Patient Rights ..................................................................................................................................... 5
Accounting of Disclosures ................................................................................................................ 6
Business Associates ............................................................................................................................. 7
Training .............................................................................................................................................. 7
Organized Health Care Arrangement (OHCA) .................................................................................... 8

RESEARCH CHALLENGES ................................................................................................................ 9

Research as Part of the Covered Entity .............................................................................................. 9
Research Sponsor Contract Language ................................................................................................. 10
Research Databases After April 2003 ................................................................................................. 12
Recruitment ....................................................................................................................................... 13
Common Criterion for IRB’s to Use to Assess Privacy Risks ............................................................ 14
Business Associate Agreements for Research .................................................................................. 14

INSTITUTIONAL DEVELOPMENT CHALLENGES ........................................................................ 15

Authorizations for Fundraising .......................................................................................................... 15
Major and Planned Giving ................................................................................................................ 15
Direct Mail and Telemarketing .......................................................................................................... 16
Miscellaneous Operational Issues ...................................................................................................... 16

EDUCATIONAL TRAINING & OPERATIONS CHALLENGES ........................................................ 18

Resident Credentialing ........................................................................................................................ 18
Students from non-covered entities .................................................................................................... 18
Students from other covered entities ................................................................................................. 18
Training graduate students ............................................................................................................... 19
Use of PHI for CME outside of the covered entity or faculty training medical students in the classroom setting (as opposed to clinical setting) ................................................................................................. 19

WORKFORCE CHALLENGES ......................................................................................................... 20

Defining the “workforce” of the covered entity (CE) for training purposes .................................. 20
When to Require a Business Associate Agreement .......................................................................... 20
Classifying and Documenting Members of the Workforce ............................................................... 21
Required Training .............................................................................................................................. 22
Tracking and Documenting the Training Effort ................................................................................ 23
Incentives for Compliance .................................................................................................................. 23
Consequences/Sanctions/Penalties Imposed for Not Complete Training on Time...................... 23

SAMPLE NOTICES .................................................................................................................................. 24
Background

On November 12-13, the AAMC and UHC hosted a conference of the membership entitled *Convergent Validity: A Forum For Academic Medical Centers to Discuss HIPAA Implementation*. The conference had over 150 attendees from many of our members. During the day and ½ meeting, the members shared their experience in dealing with the HIPAA implementation, what their issues are, and what items still need to be resolved. At the end of the meeting, the group defined five work groups to address HIPAA issues in the areas of Operations, Workforce Training, Education, Institutional Advancement, and Research. The AAMC and UHC agreed to establish a series of conference calls and a web based forum so that they could continue to move forward to issue resolution in a collaborative manner. Many items in the HIPAA regulations are ill defined. The membership believes by coming to consensus on some of these issues they can lead the implementation and guide the enforcement. What they need is a mechanism to continue their interaction.

The workgroups identified above held a series of conference calls during December 2002 and January 2003 to address specific questions that came out of the Forum. The following information is the product of those workgroups efforts. This information is the result of many individuals, those who participated in the forum, and others who facilitated and participated in the conference calls and emails. A group with diverse expertise and immense dedication to helping develop the following consensus based information. This document does not provide legal advice. Covered entities must work with their own legal counsels to address appropriate institutional requirements.

Implementation and Operational Challenges

The implementation and operations workgroup where charges with Identifying/Operationalizing Restrictions & confidential communications; Determining the Scope of the DRS; Determining what constitutes the Mental Health DRS; Operationalizing the Family Members “Safe-Harbor”; Operationalizing Patient Rights; Identifying Disclosures That Need to Be Accounted/Operationalizing the Accounting Process; Identifying BAs for reasons other than TPO; Identifying Best-Training Practices.

Restrictions

Required restrictions
(Where the patient has an opportunity to agree or object)

**Facility directory** - Some academic health centers (AHC) do not have the system capability to identify when a patient has opted-out of the facility directory, therefore, it is not reasonable to provide the patient with the ability to request that some of the information in the facility directory be restricted. If the system can identify, place a flag in the information system utilized for registration that will either warn the user of the restriction or stop the feed to the switchboard directory entirely. Limit the facility directory option to an “all or nothing” accommodation because most current systems cannot be customized.

**Clergy** - Many systems have religious affiliation field. If available, place a flag in the information system utilized for registration.

**Tracking fundraising “opt out”** - Fundraising could initiate from many areas in addition to the fundraising department (e.g. department chairpersons). Fundraising department should control the fundraising materials so that the “opt-out” patients can be tracked. (Also see section III Institutional Development.)
Accommodating requests for alternative communication - With multi-faceted OHCAs, confidential communication request should generally not be accepted at the institution level, because of the technical and administrative barriers. The approach should be to push down to the service area level for determination of the requests and acceptance only for a specific area.

A frequent request may be for certain charges not to go to the patient’s insurer, and be sent directly to the patient. Patients who request that their bills go to a different address will be instructed that the alternate address will be changed globally and not charge specific unless state laws provide otherwise. Patients who request that their insurer not be billed can also be considered self-pay and flagged as such in the system. Another might be to call at work instead of home. Patients who request that they be called at another number instead of their home number might be accommodated by putting the requested phone number in the system and not the home number. For AHCs that have many locations or are in an OHCA, requests for calls instead of appointment reminder mailings may not be easily accommodated. Some scheduling systems provide a location to insert alternate addresses to accommodate patients who request bills be sent to different addresses. If information systems cannot flag globally to call a patient instead of mailing an appointment reminder, then inform patient accommodations are limited to certain clinics/departments and not to the entire AHC’s operations.

State laws should be reviewed for minors’ and psych patients’ rights as well as laws pertaining to other sensitive information. Minors who control the disclosure of their information (e.g., STD’s) are an operational problem. The issue is if they say they don’t want their patents to know, but their parent’s insurance is paying the bill. Some AMC may choose not bill to protect the minor’s privacy.

Additional Reasonable Restrictions

Restrict all calls - The facility directory could control this restriction for AHCs that have a facility directory. The restriction may be flagged in the information system so the switchboard knows not to transfer call. Another option is to remove the phone from the room.

Restrict some calls - This request is over burdensome to some extent. A possible accommodation for some AHCs would be to instruct patient that his/her name will be taken out of the facility directory and that the patient should give the telephone and/or room number to whomever he/she wishes.

Restrict all visitors - Even though a system could be flagged to accommodate this restriction and even thought facilities have security personnel available at entrances, an AMC cannot completely guard against someone dropping in on a patient. This is not a recommended restriction to adopt. At most, AHC could agree to control on the floor by the floor personnel.

Restrict some visitors - This is over burdensome to some extent. Although difficult to operationalize, a patient could be issued a “password” and instructed to give it to his/her preferred visitors. Unit personnel would have to be extremely watchful and ensure that only those with the password entered the room. The password could be logged in an information system.

Keep identity secret - Two types of situations were discussed: 1) for “notable” types (e.g. celebrity or gang member) and 2) for those seeking genetic testing. Temporary “alias” could be created while in-house but then information would be reconciled with real patient information upon discharge. Permanent “alias” could be created but patient would be informed that all PHI collected under the alias would never be reconciled with the real patient name information. Patient would have to be considered self-pay for this accommodation. An
‘administrative alias’ in very limited circumstances could be used where only 2 or 3 people know the true identify of the patient. They are always self-pay.

Friends and neighbors access to a patient’s PHI - This is unreasonable. A concern is employees who access a ‘neighbor’s’ record, when they are not involved in their care. If the neighbor is part of the patient’s health care team, the patient should be told that all AMC personnel are bound by confidentiality and each has a duty to use and disclose only the minimum amount of PHI necessary to perform TPO and to that end, the neighbor would be entitled to perform his/her job function. If the neighbor is not involved in TPO then the AMC should reassure the patient that there are policies in place that access to PHI is for TPO only and employees who access otherwise are subject to discipline. Audits are performed by most AHC to determine access to its enterprise information systems. Patients can currently request an audit of who has accessed their records. Any suspect accesses are referred to the employee’s manager for explanation and follow-up.

**Determining the Scope of the Designated Record Set**

The Designated Record Set (DRS) may include medical/dental records, billing information, and possibly other clinical information like films, labs, ultrasounds, scans, treatment related voice conversations and emails. In providing patients access to their DRS it may be helpful to have the patient identify the records they wish to access, rather than supplying the entire DRS.

Electronic/Paper Medical Record - State statutes should be reviewed to determine if a definition for “medical record” exists. Information system should track all medical records if they are maintained in different locations. Some AHCs have different custodians of records, which may limit the ability to have one centralized record. Patients should be advised that they may have several medical records and in order to ensure that the patient gets the information needed, the patient should either present at the central medical records department or identify which records are needed.

Inclusion of emails - AHC may choose to only include “clinically relevant” emails in the record, and only when they are forwarded to the medical records department from the physician. Prescription refill requests and requests for appointments are not normally in the medical record.

Billing Information - The billing DSR needs to be defined. The following list suggests possibilities and should be considered. Medical release forms; Medicare ABN letter; Medicare life time reserve letter; Medicare notice of non-coverage letter; Payment agreement; Billing statement; Charges/adjustments/payments printout; Detail bill; Requests for amendment; Amendments; Denials of requests for amendments.

Other clinical information - Other areas that could have DRSs include: outpatient pharmacy records, clinical research records, and student health records. An AHC will need to determine if any or all of the “other clinical information” will be considered a DRS.

Some AMCs do not consider clinical data from “source departments” such as strips, graphs, and radiation therapy calibration sheets part of the DRS. An AHIMA practice brief advises that the DRS should not include source data, but that the interpretation or transcription is sufficient. To preserve source data as well as medical record information would be difficult to impossible. Exclusions: quality improvement records.

**Determining the Scope of the Mental Health DRS**

State law should be considered before determining this DRS in order to identify what should be considered part of the DRS. The mental health DRS should be separate from the main medical record. Consent must indicate that mental health records should be released.
The taskforce discussed this response to comments received from HHS: “The final rule makes it clear that any notes that are routinely shared with others, whether as part of the medical record or otherwise, are by definition not psychotherapy notes, as we have defined them.” One operational approach is that psychotherapy notes must be distinctly separated from all other records and only grouped with other psychotherapy notes.

**Shadow Records**

All organizations have Shadow Records to varying degrees and they present an operational problem in providing patients with a complete copy of their record. No one has a short-term solution to Shadow Records. Long term, scanned records can provide rapid access to the legal record and reduce the need for Shadow Records in ambulatory settings. Stanford has been scanning all records for the last five years and has significantly reduced the number of Shadow Records in the last few years.

Shadow records if they exist and contain information that is separate from the medical record should be considered a part of the DRS. However, there are concerns about the medical records department’s ability to identify and track these records. Many times the medical records department does not know of them until a patient contacts medical records to say that he/she didn’t get all of her information and indicates that a physician file may contain additional information. Policies should address the use of shadow records and communication with the medical records department. Shadow records are not recommended.

**Operationalizing the Family Members “Safe Harbor”**

The regulation provides reasonable options in this area. “Information about the patient may be given to a family member or friend of the patient if the patient: 1) agrees by either being present at the time just prior to the conversation with the family member and/or friend and has verbally agreed; 2) has not objected after being provided the opportunity; or 3) it can be reasonably inferred from the circumstances, using professional judgment that the patient does not object to providing the family member and/or friend with the patient’s information. In an emergency situation, professional judgment may be used to determine if the disclosure would be in the patient’s best interest. Include the Rule’s suggested solution for this requirement in the training process.

To assist patient understanding AHC could advise patient in Notice of patient’s duty to identify which visitors should not have access to information. Other suggested alternatives: document in either the consent form or the medical record who can receive care information; limit the information to that which is contained in the facility directory; information system could indicate who the “primary contact” is and that is the only person who receives information about the patient; a code name or password could be used.

**Patient Rights**

Privacy Notice - There is still a basic tension between making the Notice as patient friendly as possible and having a document that can be defended in court. Some institutions are using a layered Notice and others are not. Some Notices are 3 or 4 pages and others run to 7 or 8 pages. There was no general agreement on what needs to be explained in the section on ‘disclosures without your authorization’. Some organization feel they need to enumerate most or all of the public health disclosures and others are using a fairly terse summary statement.

Examples (will be on the web)
Amend Record - Most organizations are focusing this process in their information systems and billing office organizations. Many organizations are considering any request to change data in the designated record set a request to amend. This includes changes of address and other contact information.

Accounting of Disclosures
If information is being disclosed outside the Entity and the disclosure is not for the Entity’s use, then the disclosure is not part of TPO. This view would require accounting for most public health disclosures. Health care oversight may generally be viewed as part of TPO. Accreditation disclosures to organizations like the ACS are still open to interpretation. Some institutions are treating all research as a disclosure, since the hospital is not part of the University. Others are logging preparatory to research disclosures to cross check against their security audit functions.

This area is still a major operational challenge for most institutions. Operationally, everyone is facing the challenge of getting a handle on a decentralized process that now needs a centralized accounting mechanism. Many organizations are looking at web-based solutions for capturing data about disclosures.

One organization is building an in-house solution that addresses patient ID issues across their enterprise. Another is building an in-house web based solution. Several are evaluating vendor solutions.

Example

(Oregon Health Science Center Accounting for Disclosures)
45 CFR 164.528 provides that an individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- To carry out treatment, payment and health care operations;
- To individuals of protected health information about themselves;
- Incident to a use or disclosure otherwise permitted or required by this subpart;
- Pursuant to a valid authorization;
- For the facility's directory or to persons involved in the individual’s care or other notification purposes;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials;
- As part of a limited data set; or
- That occurred prior to the compliance date.

Examples of Disclosures that have been identified that would require an accounting:

1. To Health Services/Public Health as required by law or pursuant to Health Services/Public Health survey authority, including:
   a. Infectious disease reporting
   b. Fetal death
   c. Birth certificates
   d. Death certificate
   e. Teen suicide
   f. Intimate Partner Violence survey reporting
   g. Newborn Screening (PKU)
   h. Oregon Death with Dignity (OR specific)
   i. Reports of Death for purposes of organ donation
   j. Poison Control

2. To State Medical Examiner, such as reporting of gunshot wounds

3. To coroners and funeral directors

Results of Convergent Validity Workgroups March 2003
4. To Advisory Boards, such as the State Trauma Advisory Board
5. Disclosures made as a result of a subpoena or court order.
6. To organ, eye, or tissue donation agencies or disclosures for transplantation purposes
7. To Registries, external to the entity and mandated, including:
   a. Cancer Registry
   b. Immunization Registry
   c. Trauma Registry
8. To Department of Human Services or law enforcement regarding elder abuse or child abuse
9. To and by business associates, unless disclosure is for exempt purpose
10. To Department of Motor Vehicles
11. To Health oversight agencies such as Department of Human Services acting in their role as a regulating agency, such as disclosures for purposes of audit. Notably, disclosures to JCAHO need not be accounted for.
   a. CMS
   b. OHRP
   c. DHHS
12. To investigators, mental health examiners and the court for purposes of mental commitment (Hospital Holds for Mental Health)
13. To law enforcement, unless 1) disclosure is made pursuant to authorization; or 2) law enforcement has requested that accounting not be provided for a specified period of time
14. Related to research disclosures performed with a waiver of authorization (unless only limited data set information is disclosed), preparatory to research, or on PHI of decedents. Note: if the researcher is an employee these are qualified uses and are not disclosures and therefore do not require an accounting. Only when the information leaves the entity, such as if a researcher outside the covered entity does these activities or when the PHI is sent to the Sponsor, does the PHI become subject to the accounting rule.
15. To State Crime lab, if 1) specimen is accompanied by a label with protected health information on it; and 2) release is performed without authorization
16. To the Food and Drug Administration for purposes related to the quality, safety or effectiveness of a FDA-regulated product or activity.

**Business Associates**

Institutions should have or be building and inventory of contracts that will require Business Associate Agreements (BAA). Some organizations have more decentralized contracting functions and creating an inventory is proving to be a challenge. Several organizations are reviewing their general ledger to see who is being paid, but might not have a BAA agreement. Ideally, centralized contracting processes make the BA agreement process that much easier.

There was no discussion about standard language most organization’s chief counsel has crafted language.

**Training**

Most organizations are planning to train their entire workforce. Some organizations are also planning to train BA’s that are on-site on a regular basis. Everyone is talking about having to train 1000’s of people. Most organizations are putting the responsibility for training compliance on their managers. Many are evaluating or using some form of web/computer based training for their basic training. Some are treating physician basic training as a special case. Multiple approaches are in the works for training special areas like registration, medical records, and researchers. Loyola is using a train-the-trainer approach. MCG is putting an emphasis on developing scripted answers for common questions. Community and visiting physicians are being handled with a variety of approaches. OHSU and Stanford are treating all physicians (faculty and community) who have privileges as part of the workforce. Others are a closed practice and have a relatively small number of MD to train. HIPAA language is also being incorporated into job descriptions.
Organized Health Care Arrangement (OHCA)

An OHCA requires either clinical or operational integration. The OHCA requires clinical integration to be a “clinically integrated care setting in which individuals typically receive health care from more than one health care provider.” Integration on the basis of faculty appointment, or mandate to participate in a faculty practice plan may be sufficient to qualify entities as an Affiliated Covered Entity (ability to control), but does not, satisfy clinical or operational integration.

Clinically integrated means: mutual patients (not others in other facilities); share same information about the same patients in the same patient database; mutual patient information in different databases. Same medical records; hold faculty position status (could also fit in operationally integrated definition). Physicians are credentialed at the hospital facility; consider factors to the left to determine if the AMC and its OHCA partner(s) meet the criteria.

Operationally integrated means: holding both (or more) entities out as one; shared managed care contracting; Holds faculty position status (could also fit in clinically integrated definition); one notice of privacy practices.

Some AHC are using a “Care Episode/site” based definition: Clinical integration is site-based integration (i.e. a hospital setting), where multiple services on the Medical Staff, nurses, and other health care practices provide care to the individual. During a visit to the hospital, the OHCA and the joint notice covers both the provider’s and the facility’s/hospital’s privacy requirements for that visit. However, if the health care provider follows up with the patient in their private practice, the provider and facility/hospital are not longer in an OHCA.

Qualification as an OHCA should be determined after reviewing all of the issues. It is important that the scope of the OHCA is noted appropriately in the OHCA’s notice (e.g. limited to hospital in OHCA and not other hospitals at which the physician may practice).

Some OHCA configurations

Examples
AMC #1 included hospital and clinics but carved out SNFs, Dept of Corrections and dental foundation.
AMC #2 included hospitals, clinics and campus health functions in OHCA
AMC #3 included hospital and clinics (Corp 1), physician foundation (Corp 2) and school of medicine students and research (Corp 3) in OHCA but excluded other university related health functions (Corp 3).
AMC #4 – included inpatient and outpatient facilities, a physician practice, ancillaries, school of medicine, school of dentistry, and school of nursing clinics.
Research Challenges

Research as Part of the Covered Entity

There has been a great deal of discussion among AHCs as to whether to include research activities within the CE and if so, what part of the research enterprise should fall within the CE. The question seems to be how to draw the boundaries within an institution’s research activities segregating certain types of research as falling within the CE and excluding other research from the CE. In the research taskforce we explored the advantages and disadvantages of including research in the cover components of the hybrid entity. We are all dealing with this issue somewhat differently.

Reasons NOT to include research in the CE:
Research is not a covered function under HIPAA
Some researchers are not covered healthcare providers i.e. are not “billing”
Many schools don’t bill electronically for research procedures
Whether or not to include research in the CE is immaterial because AHCs would have to do the research regulations for HIPAA anyway so privacy is already going to be protected

Reasons to include research in the CE:
In AHC most patient-oriented research is conducted by physician-researchers so the clinical and research aspects of the physician are too closely aligned to draw distinctions.
Many clinical databases are also used for research purposes.
If research isn’t part of the CE then we are required to put “Firewalls” between the clinical and research activities. Firewalls include technical segregation of clinical and research data as well as “behavioral firewalls” to segregate clinical and research activities within a clinic or within an individual’s practice.
Some schools are billing third parties for research procedures as is permitted under certain circumstances by the National Coverage Decision.
Casting a broader net across the AHCs research activities is necessary because there are many basic scientists that are co-investigators with clinicians on human studies.
HIPAA privacy practices are really “best” practice therefore applying privacy HIPAA standards to research activities is a good idea whether or not HIPAA explicitly requires it.

Each entity is going to have to make its own decision about whether or not (and to what extent) research is part of the covered component. It seems that HIPAA gives AHCs some latitude to include non-covered health care providers. One of the considerations that will impact this decision is the “legal” structure of the AHC for example are hospitals under common ownership & control of the University, is the Physician Practices under common ownership & control, what is the nature of the relationship of the physicians to the CE – employee, contractor, other.

Defining “Covered” Research: To answer the question which areas of research should be covered by HIPAA. This can be achieved in a three of different ways.

Organizational Unit Method: This may be achieved by including specified organizational units in the health sciences as the Schools of Medicine, Nursing, Dental and Public Health.

Clinical vs. Basic Science Method: Another method is to designate individual faculty or certain labs as being part of the covered entity such as including clinical faculty and excluding basic science faculty.

Project Method: A third option is to consider whether or not HIPAA applies on a “per project” basis such as only including research that includes the provision of health care in the CE and research that...
does not include the provision of health care is outside of the CE. Another method would be to include research that either creates or accesses IIHI. OCR guidance clarifies that if the study involves the delivery of routine health care, then the project must be covered under HIPAA.

Structural Considerations:

Administering Patient Rights: If research is considered part of the CE then it needs to behave like part of the CE. For example the CE is required to provide the Notice of Privacy Practices, if research is part of the CE then this notice must also be made available to research participants.

The Notice of Privacy Practices must be given if the study involves the delivery of routine health care. If the consent/authorization references the NPP, then the NPP must be delivered during the consent process. At minimum the NPP must be delivered when the research subject participates in the routine health care activities of the study. *The only place that refers to the NPP is in the steps for revoking authorizations. If the consent/authorization describes the revoking process, then the NPP reference is not needed.*

Designated Record Set: If research is considered part of the CE do research records become part of the designated records set? The group seems to feel that it is not part of the designated records set to the extent that these records are kept separately from the patient chart. The December 2002 OCR guidance clarifies that it is unlikely that a researcher would be maintaining a designated record set. Workgroup members caution that institutions must assure that any treatment information generated in the research context does indeed become part of the medical record.

Accounting for Disclosures: If research is not part of the CE then any researcher access of PHI under a waiver of authorization becomes a “disclosure” requiring an accounting. By including research within the CE much of this activity may be considered a “use” rather than a “disclosure” which may minimize the accounting burden. Also, the entity should closely consider the CE structure with regard to this area. If the medical center is under common ownership, and if research is deemed a covered component of the entity, access for research purposes under a waiver could be considered a “use.” However, if hospitals and physician practices are separate legal entities, access through a waiver becomes a disclosure that requires tracking, even if the entities have formed an OHCA. In order to meet the accounting requirement under HIPAA researchers will need to understand the difference between a “use” and a “disclosure” so it will be necessary to draw these distinctions as clearly as possible.

Training: If research is part of the CE than all of the researchers and staff will need to meet the HIPAA training obligation prior to April 14, 2003.

Criminal & Civil Penalties: Including research in the CE and expanding HIPAA beyond the minimum that the law allows also expands the potential institutional legal liability of HIPAA fines and penalties.

Research Sponsor Contract Language
While it may be desirable for AAMC to approach Pharma with standard contract language, those discussions may not happen during the early phases of HIPAA implementation. The contract issue is that HIPAA requires the explicit statement that once PHI is disclosed in the context of research it is no longer covered by HIPAA. Many of the AHC’s believed that the lack of protection is insufficient for our research subjects. Although a BA agreement or data use agreement may be “too much” and objectionable to Pharma, some sort of patient privacy language should exist. Many AHCs are developing their own contract language to protect the privacy of information provided to Sponsors. Workgroup members discussed the goal that the research contract should bind the sponsor to the terms of the authorization.

Results of Convergent Validity Workgroups March 2003
Three examples are provided below:

SAMPLE 1

“In the event the Sponsor shall come into contact or otherwise have access to Study subject’s medical records, the Sponsor shall hold in confidence the identity of the subject and shall comply with all applicable law(s) regarding the confidentiality of such records. Sponsor will review and approve of the Informed Consent document and any authorization document. Sponsor agrees that, should the Sponsor gain access to any protected health information of Study subjects, sponsor will treat such protected health information in accordance with the Informed Consent document, any Authorization document, and all applicable laws and regulations. If Sponsor gains access to any protected health information that is not covered by the Informed Consent or Authorization, Sponsor shall hold such information in the strictest confidence, shall not remove records containing such information from the institution and, if inadvertently removed, shall immediately return any records containing such information to the institution.”

SAMPLE 2

HIPAA

NOTE: Change the identifiers of the parties to whatever is used in the contract; in the instance below, "State" is us . . . "Contractor" is the other party. For clinical trials, "Contractor" will be "Sponsor" or "CRO" and "State" will be "State Name" or "Institution."

“HIPAA Compliance.
Contractor warrants to the State that it is familiar with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations, and will comply with all applicable HIPAA requirements in the course of this contract. Contractor warrants that it will cooperate with the State in the course of performance of the contract so that both parties will be in compliance with HIPAA, including cooperation and coordination with State privacy officials and other compliance officers required by HIPAA and its regulations. Contractor will sign any documents that are reasonably necessary to keep the State and Contractor in compliance with HIPAA, including but not limited to business associate agreements.

“Confidentiality of PHI Records.
Strict standards of confidentiality of private health information (PHI) records and information shall be maintained in accordance with applicable state and federal law. All PHI material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State shall be regarded as confidential information in accordance with the provisions of applicable state and federal law, state and federal rules and regulations, departmental policy, and ethical standards. Such confidential information shall not be disclosed, and all necessary steps shall be taken by the Contractor to safeguard the confidentiality of such material or information in conformance with applicable state and federal law, state and federal rules and regulations, departmental policy, and ethical standards.

"The Contractor's obligations under this section do not apply to information in the public domain; entering the public domain but not from a breach by the Contractor of this Contract; previously possessed by the Contractor without written obligations to the State to protect it; acquired by the Contractor without written restrictions against disclosure from a third party which, to the Contractor's knowledge, is free to disclose the information; independently developed by the Contractor without the use of the State's information; or, disclosed by the State to others without restrictions against disclosure. Nothing in this paragraph shall permit Contractor to disclose any information that is confidential under federal or state law or regulations, regardless of whether it has been
disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties.

"It is expressly understood and agreed the obligations set forth in this section shall survive the termination of this Contract."

SAMPLE 3

Definitions: Individually identifiable health information (IIHI): see 45 CFR section 106.103.

All individually identifiable information transmitted to the sponsor is considered IIHI. The information remains IIHI unless it is de-identified using the procedures specified by 45 CFR section 164.514(b). IIHI cannot be used by the sponsor except as follows.

IIHI may be used by the sponsor for any purpose directly related to the proper conduct of the research project, including accumulation of results, auditing of research integrity, and reporting to appropriate governmental agencies. In addition, IIHI may be used with respect to an FDA-regulated product or activity for which (the study sponsor) has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:
(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
(B) To track FDA-regulated products;
(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or
(D) To conduct post marketing surveillance.

Research Databases After April 2003

Who “holds” the databases – the CE, the faculty provider, the researcher? How do you locate all databases in the CE? Though the charge for the taskforce was research, the discussion broadened to databases in general; it is difficult to determine intent of the data as they sit.

The CE is liable for the databases under HIPAA, but it is individuals who actually work with them that are responsible for the integrity and tracking of the data use. To that extent, the CE, faculty, and researchers are all holders of data. Some collect and maintain the database itself and others are recipients.

Two areas seemed most troubling from the liability perspective of HIPAA:
Case logs held by individuals (usually physicians), often with no apparent purpose for their collection.
Databases collected for future, unspecified, research, and not already addressed by an IRB. These two often overlapped.

Case logs are often held, particularly by residents in surgery and sub-specialty areas that are highly technical (cardiology, GI, etc.) for submission to their specialty boards as part of the board certification process. As such, this is an operations activity (not research). Concerns were expressed about the security of the data (often on PDAs or personal systems) and that the PHI leaves the CE’s control when the provider does (finishes training). Additionally, a number of providers submit cases meeting particular characteristics to national registries (sometimes without any formal agreement at all); these will need Business Associate Contracts or Data Use
Agreements depending on the registry intent and extent of identifiability of the data submitted and may need IRB involvement.

Databases collected for unspecified research need to be identified and appropriately addressed with the governing IRB. The holders need to be educated in the current regulations and obtain waiver of consent/authorization or start getting consent/authorization as appropriate to the circumstances. This is a concern under current regulations as well as for HIPAA.

Finding the databases is both an education activity and a technical one. Equipment on the AMCs network can be scanned by network tools (i.e. SMS and WRQ Express) for files of particular types to identify potential databases. Some institutions are performing a survey of research servers to locate these files, and labeling the servers on which they are located as “critical hosts” in preparation for the security requirements to be mandated by the Security Rule.

Though there are the penalty risks as stated in HIPAA, the major risk of HIPAA violations is the public impression of our institutions. Education of the faculty and other researchers may be the best defense. Providing support to help them become compliant will also help.

Creating a database that includes PHI - Databases created for future (unspecified) research are allowed under HIPAA. Depending on the circumstances, either an authorization or waiver will be required to assemble the data and a waiver for the analysis. If the database is kept inside the CE, its contents are likely to be subject to the other security and privacy requirements of HIPAA.

Permissible uses for the databases - Databases are acknowledged to have multiple purposes. For research, the uses are regulated by the activities specified in the waiver or Data Use Agreement (DUA). Changes to the goals require new/amended waivers or DUAs.

Researcher access the database - Through the IRB. The researcher will need obtain approval from the IRB via a waiver of authorization to access the information for research purposes.

IRB or Privacy Board approval - Approval is needed everywhere that the information is not de-identified and/or anonymized.

Recruitment

When a researcher/provider does not have a treatment relationship to the individual, you cannot approach the individual to participate in the study without the individual’s authorization. Time sensitive research studies – e.g. neonates – how can we implement the contact with the individual in a timely manner? Solution: Treatment team or someone expected to know the situation may contact the patient representative.

Although certain areas of research may not be covered by HIPAA some of the organizations felt that the privacy of IIHI information should still be emphasized. In fact many believe that this is already required as part of the Common Rule. As an example, for health sciences research an entity may want to develop a prioritized list of individuals who can contact a patient to request that they participate in the study. (*The new standards for privacy issued by DHHS suggest that if health sciences research (or other types of research) is outside of the CE ONLY someone with a direct treatment relationship with the patient may contact the patient to solicit participation – although if it is inside than anyone within the CE may make the initial contact with the subject.*)

An example of recruitment strategies is provided below:
“Solicitation using PHI (see “For Identification of potential subjects” for IRB waiver requirements)

Contact methods in descending order of preference, are:
By a physician or other licensed independent practitioner who has taken care of the patient,
By UCDHS, using a cover letter and script approved by UCDHS, or
By the researcher
Direct recruitment by a researcher who has not taken care of the patient will require UCDHS approval
and will only be allowed when both the other two alternatives are impractical.”

Solicitations that do not use PHI:

Contact methods that do not start by identifying particular patients are acceptable if approved by the IRB
Examples of such methods are: flyers posted in clinics, advertisements in mass media, and mailings that
do not use any information, including demographic information, collected by UC Davis Health System.
Mailings that are based on patient lists do use PHI and require IRB waiver of authorization for at least
the recruitment phase of the protocol. These mailings are further subject to the conditions under
“Solicitation using PHI”.

The group discussed the option of using the “preparatory to research” provision for the purposes of study
recruitment. OCR guidance confirms that this provision can be used for recruitment, provided the researchers
are part of the covered entity. However, several group members were uncomfortable with using this provision
for recruitment, endorsing waiver of authorization for recruitment as the safer and preferred option.

Common Criterion for IRB’s to use to Assess Privacy Risks
Develop a list for routine uses and disclosures and MNS for non-routine uses and disclosures; define teaching;
define research. Per the discussion we have not yet created standards for research under HIPAA privacy.

Business Associate Agreements for Research

The workgroup discussed requirements and guidance on obtaining business associate agreements (BAAs) from
researchers. We agreed that if an outside researcher is performing a duty that rightfully belongs to the covered
entity, then a BAA is required. Stripping PHI of identifiers to create a de-identified or limited data set would
fall into this category.

Some institutions employ an outside entity to develop data for a clinical trial. Assuming individual
authorization had not yet been obtained, a business associate agreement would be required for this activity.
Institutional Development Challenges

The Institutional Development workgroup designed a short survey to assess members’ fundraising scope as well as learn more about individual institutions’ approaches to implementing HIPAA. The medical fundraising enterprise at responding institutions is largely an independent administrative unit or a division within the university’s larger development office. A small number are separately incorporated foundations that are part of the Covered Entity or a separately incorporated foundation that is not part of the Covered Entity. Most respondents owned the medical center affiliated with their institution. About a quarter do not own the medical center and another quarter have both conditions. Respondents were spread across an annual medical fundraising range with most in the $1M - $100M range. In preparing for HIPAA most institution’s level of HIPAA readiness (related to fundraising) includes having some policies and procedures in place. Only one institution indicated they were ready to operationalize their HIPAA planning.

Authorizations for Fundraising

Most institutions plan to seek written authorization for fundraising only when necessary on an as hoc basis. A few will seek authorization at admission for all patients. The vehicle for written authorization for fundraising will be a stand-alone form exclusively for fundraising authorization. When an ad hoc written authorization needs to be obtained most institutions will require the physician to obtain verbal consent from the patient for a designee (nurse, administrative staff member, development officer, etc.) to obtain the written authorization. However, several institutions indicated they are not yet sure how they will manage this process. Most institutions are still unclear when a written authorization for fundraising will expire. The average length from respondents was 1-5 years. The office of record for written authorizations for fundraising will most often be the development office/foundation followed by the medical center records department.

Major and Planned Giving

Members were split on a physician speaking directly to a patient about making a gift. Half indicated the physician could, but only to seek a general (not disease-specific) gift to the institution unless a written authorization is on file, and the other half indicated the physician could discuss any gift opportunity (general or disease-specific) without written authorization. Members were again split on a physician sharing the name of a patient with the development office/foundation. Half indicating this is not possible unless a written authorization is on file, and the other half said regardless of the physician’s specialty or the patient’s location in the facility the physician could share the patient’s information.

A physician and/or a development office/foundation staff member providing a fundraising volunteer or campus administrator (dean, CEO, etc.) with the name of a patient is not possible without a written authorization on file. Also a list of a physician’s patients may not be “rated and screened” by the physician, development office/foundation staff members, fundraising volunteers and campus administrators (dean, CEO, etc.) without a written authorization on file for each patient.

The development office/foundation may not ask for the name of the physician (and by extension division and department) of a newly admitted patient who is believed to have major gift capacity unless a written authorization is on file. A planned giving officer may not ask for the name of the physician (and by extension division and department) of a decedent to help determine an appropriate designation for an undesignated bequest unless the executor of the decedent’s estate provides written authorization.

A researcher cannot (i.e., a faculty member who is not a direct care provider) access patient records for fundraising purposes unless a written authorization is on file for each patient and the researcher is part of the Covered Entity.
The development office/foundation staff may have access to daily lists of patient admissions only for patients with a written authorizations on file or as long as only demographic information is viewed.

**Direct Mail and Telemarketing**

An individual physician may not send a fundraising letter (independently or with assistance from the development office or foundation) to a group of his/her patients unless written authorizations are on file for every recipient or as long as disease, diagnosis, procedure, etc. are not used to refine the data pull.

A clinical division may not send a fundraising letter (independently or with assistance from the development office or foundation) to a group of patients unless written authorizations are on file for every recipient or as long as disease, diagnosis, procedure, etc. are not used to refine the data pull.

A clinical department may not send a fundraising letter (independently or with assistance from the development office or foundation) to a group of patients unless written authorizations are on file for every recipient or as long as disease, diagnosis, procedure, etc. are not used to refine the data pull.

Disease, diagnosis, procedure, physician name, division, department and/or other non-demographic information may not be used to exclude groups of patients from solicitations unless written authorizations are on file for every patient in the group to be excluded.

Members believe the HIPAA regulations related to direct mail fundraising apply equally to tele fundraising.

HIPAA does not allow the development office/foundation to send a file of patient data to companies such as Target America, Wealth Engine and Marts and Lundy for prospect (wealth) screening unless written authorizations are on file for every patient in the file or as long as the selection criteria is based only on demographic information.

**Miscellaneous Operational Issues**

The development office/foundation may not request a list of a physician’s patients from the medical records (or similar) department, unless the list contains only demographic information or only the names of patients who have written authorizations on file.

The development office/foundation may not request a list of the patients seen in a division or department from the medical records (or similar) department unless the list contains only demographic information or only the names of patients who have written authorizations on file.

A development office/foundation may not add a patient’s name to the VIP/Concierge Service list and subsequently provide upgraded patient services (e.g., flowers, special food service, room upgrades, visits from the dean/CEO, etc.) unless a written authorization is on file or as long as the provision of upgraded patient services does not reveal the name of the patient’s physician; his/her disease, diagnosis, procedure, etc.; or his/her location in the facility if the location divulges similar information.

A development office/foundation may not target patients on its VIP/Concierge Service list with fundraising communications unless written authorizations are on file for every recipient or as long as disease, diagnosis, procedure, etc. are not used to refine the data pull.

At most institution, the office of record for fundraising "opt outs" will be the development office/foundation.
Members were not clear about what steps must be taken to secure PHI that a development office/foundation has obtained before April 2003. Some indicated that no steps are needed because, PHI obtained before April 2003 is “grandfathered.” Others believe all PHI—other than demographic information—must be purged unless a written authorization is obtained.
Resident Credentialing

Covered entities must make PHI available to Accreditation boards for resident credentialing. The task force developed to approaches to this issue.

1. Credentialing boards will be considered BAs. The covered entity will be responsible for tracking those disclosures
   -OR-
2. Limited Data Set with data use agreement. The covered entity will not have to track these disclosures. The covered entity will need to negotiate a Data Use Agreement with the outside entity.

It was suggested that to assist member ACGME and ABMS (American Board of Medical Specialties) as well as AAMC develop a best practice for release of information for resident accreditation. A consensus must be established as soon as possible.

Students from non-covered entities

Students come to an AMC from a variety of other schools and organizations such as from a technical school/community college.

Students (not of the covered entity) taking PHI back to their institution:

Students should bring information in a limited data set. Data use agreements must be in place.

Faculty visit the covered entity to supervise their students:

Business Associate Agreements should be in place.

Faculty from an outside institution come to the covered entity to teach/demonstrate a procedure:

The faculty is likely exposed to PHI. Visiting faculty in this situation should be considered part of the covered entity’s workforce and part of the provider module. As such, the covered entity should be able to demonstrate that the visiting faculty has received the covered entity’s HIPAA training and is aware that the minimum necessary standard applies. The outside faculty should not be allowed to use or disclose the University patient’s PHI outside of the University for any purpose (except with patient authorization), other than treatment of the patient or payment for such services.

If affiliated institutions use the same/similar methodology/materials in training their workforce then training should be transferable to affiliated institutions (for community physicians, residents while traveling to affiliated institutions).

Students from other covered entities

Agreements for students to come from another covered entity to your institution for training purposes usually involve an affiliation agreement.

Affiliation Agreements:

1. Insert BAA language into affiliation agreements;
   -OR-
2. Students from affiliated organizations, once inside the covered entity, should be considered part of the workforce and may use PHI for clinical teaching purposes. The Notice of Privacy Practices and Affiliation Agreement must contain language that describes the use and disclosure of PHI for teaching purposes. Should students need take PHI back to their affiliated organization a Limited Data Set must be used and a Data Use Agreement be in place. Students should receive specific
HIPAA awareness training on policies that impact their area of contact in the covered entity; Students should be able to document that they have received general HIPAA awareness training from their home institution (e.g. produce a certificate).

- OR-

3. When two covered entities have a teaching relationship to a patient, and there is an affiliation agreement in place for teaching purposes, the student of either institution may use PHI freely – so long as: 1) the relationship to the patient is teaching; 2) the minimum necessary applies; 3) The Notice and Affiliation Agreement include appropriate language describing the use and disclosure of PHI between two covered entities for teaching purposes when both covered entities have a teaching relationship to the patients; and 4) students have received comparable HIPAA training as determined by the Privacy Officer.

Training graduate students

1. All students, faculty, and staff of schools that define themselves as part of a unified covered entity such as an OCHA, SACE, etc should be treated as employees for HIPAA purposes.

   -AND-

2. Schools outside the unified covered should be treated as we would any technical school, community college, outside medical school, etc. and should require that the equivalent of a BAA be in place or, if PHI is removed from the covered entity as part of the student’s curricula, a Data Use Agreement should be in place allowing for the use and disclosure of a Limited Data Set.

Use of PHI for CME outside of the covered entity or faculty training medical students in the classroom setting (as opposed to clinical setting)

Consensus:
Use of PHI for these purposes require either Authorization by the individual or a Data Use Agreement. PHI used and disclosed for CME purposes is not operations. The covered entity may want to engage in a Data Use Agreement with the CME division.
Workforce Challenges

Defining the “workforce” of the Covered Entity (CE) for training purposes

(Note: “Workforce” is defined by 45 CFR 160.102 as “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.”)

Most institutions included the following in their workforce definition: students from an institution outside of the CE; Visiting professors; Volunteer faculty involved in teaching, but not clinical care for the CE; Volunteer faculty involved in teaching and clinical care for the CE; VIPs and guests; (i.e. donors learning more about the organization); Vendor reps.

Reference to other Relevant Provisions: A “business associate” includes an individual or entity that is not a member of the “workforce” of the CE, but provides services on behalf of the CE to perform a covered function, and the services involve the “disclosure of individually identifiable health information.” 45 CFR 160.103.

“Disclosure” means “the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.” 45 CFR 164.501.

Comments to the regulations note, “a hospital may enlist the services of another health care provider to assist in the hospital’s training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.” 53252.

Define “workforce” broadly, excluding vendor reps, guests and VIPs. This allows individuals to access PHI while they are on-site.

The problem is what to do with students who are part of “workforce” when they access PHI, but want to take PHI back to institution that is not part of the CE. Professors at non-CE institution are not part of CE workforce.

Do CEs plan to require BA agreements with those institutions?

Solution one: BA agreement between hospital and training institution.

Solution two: OCHA between two covered entities that are working together to educate students.

When to Require a Business Associate Agreement

A business associate agreement should be obtained for the following relationships: Vendors, VIPs, guests, task force recommends BA agreement.

(Note: 1 year delay may impact handling students on rotations in small community offices)

Sponsoring institutions may want to provide the community volunteer faculty with the CE’s training modules, and other HIPAA materials prior to April 2003. Ask that they complete training by April 2003. Offer to allow them to use training for physician’s own clinical office staff for training.
Only require the physician participating in the training of the student to undergo HIPAA training if part of the workforce of the CE.

**Classifying and Documenting members of the workforce**

Approaches: Role based analysis. Identify category of access needed on a department-by-department basis. Will likely need to look at particular function of the individual in the position. Review access to paper and electronic records, and level of detail needed to perform job function (i.e. scheduling clerk versus treating care provider). Look at authority to disclose information, view information, create documents, change or amend documents. Ask supervisors to describe what degree of access is necessary for each position. Specify clinical or research function. Determine HIPAA education based on level of access. Develop mechanism to document electronically.

**Example**

*PHI Access Levels and Definitions*

**Level 1:**

Position's primary responsibilities do not include use and disclosure of and requests for, “Protected Health Information (PHI).” However, administrative support functions crucial to the success of the business may require, but are not limited to, exposure to PHI for the purpose of organization, storage, transportation and confidential destruction.

**Level 2:**

Position is involved in “Treatment,” “Payment,” and or “Health Care Operations” (Commonly referred to as “TPO”).

Position is involved in “Treatment” as defined: Treatment refers to the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to the patient; or the referral of a patient for health care from one provider to another.

**And or**

Position is involved in the “Payment” process as defined: Payment refers to: 1. The activities undertaken by: (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and 2. The activities in section (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to: (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) Risk adjusting amounts due based in enrollee health status and demographic characteristics; (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care or justification of charges; (v) Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and (vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to reimbursement: (A) Name and address; (B) Date of birth; (C) Social security number; (D) Payment history; (E) Account number and (F) Name and address of health care provider and/or health plan.

Results of Convergent Validity Workgroups March 2003
And or

**Position** is involved in "**Health Care Operations**" as defined: Refers to any of the following activities of the covered entity to the extent that the activities are related to the covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates: 1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; 2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities; 3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 164.514(g) are met, if applicable. 4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; 5. Business planning and development, such as conducting cost-management and planning-related analysis related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and 6. Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsor, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; (iii) Resolution of internal grievances; (iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity, or following completion of the sale or transfer, will become a covered entity; and (v) Consistent with the applicable requirements of 164.514, creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in 164.514(e)(2).


**Required Training**

Institutions are offering a variety of training formats including online, lecture based, reading a handbook, and a combination of all of these formats. They are also providing different levels of detail in the training similar to the listing below.

Options include:

- Level 1: incidental access—housekeepers, nutrition care workers, ancillary personnel
- Level 2: scheduling clerks, customer service personnel with limited access to PHI
- Level 3: individuals responsible for disclosing PHI for non TPO (responding to subpoenas, requests from patients)
- Level 3: faculty members, direct care providers
- Level 4: researchers
- Level 5: “train the trainer”
The basic level of training averages between 30-45 minutes. Physicians/Professional training averages 60-180 minutes. Most institutions will require individuals taking the HIPAA training to obtain at least 70 – 80% correct answers to pass.

**Tracking and documenting the training effort**

Institutions are using computerized tracking, attendance sheets, HR database, and department responsibility. Most institutions are rolling HIPAA training into new hire orientation that takes place within 4 – 8 weeks are hire. Individuals will need to update training yearly.

**Incentives for compliance**

Most members did not indicated any incentives in place one example was: “Mystery shoppers” in work environments—ask questions and hand out candy bars for correct answers. “Harry’s Hernia” gentle reminders about privacy in elevators, cafeteria, public areas. Rewards for departments with full compliance by certain dates.

**Consequences/sanctions/penalties imposed for not complete training on time**

Most common penalties for individuals that do not complete the training include:
- Staff—disciplinary action
- Restrict privileges (similar to failure to complete medical records)
- Utilize existing mechanisms for imposing sanctions on faculty members
- Researchers—IRB will not consider protocols or renewals

These were followed by:
- Lock out of email
- Lock out of electronic medical record
- Report to Dean/Department Chair—faculty code violation/old off departmental funding
- Hold paycheck
- Students—deny clinical rotations, student code violation
NOTICE OF PRIVACY PRACTICES

Effective Date: 14-April-2003

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

OUR PLEDGE TO PROTECT YOUR PRIVACY

Stanford Hospital and Clinics (SHC) and Lucile Packard Children’s Hospital (LPCH) (the “Hospital” for purposes of this notice) know that medical information about you is personal, and we are committed to protecting the privacy of your information. As a patient of the Hospital, the care and treatment you receive is recorded in a medical record. So that we can best meet your medical needs, we share your medical record with all the health care providers involved in your care. Only to the extent necessary, we share your information to conduct our business operations, to collect payment for the services we provide to you and to comply with the laws that govern health care. We will not use or disclose your information for any other purpose without your permission.

We are required to:

- Make sure that your medical information is kept private;
- Give you this notice of our legal duties and privacy practices with respect to medical information about you; and
- Follow the terms of the notice that is currently in effect.

We have a responsibility to safeguard the privacy and integrity of your records. This Notice explains our privacy practices and your rights regarding your medical information.

WHO WILL FOLLOW THIS NOTICE

The following individuals share the Hospital’s commitment to protect your privacy and will comply with this Notice:

- Any health care professional authorized to enter information into your medical records.
- All departments and units of the Hospital, including our outpatient clinics.
- All employees, volunteers, trainees, students, contractors and medical staff members of the Hospital.

YOUR RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU

You* have the following rights regarding your medical information:

RIGHT TO INSPECT AND OBTAIN A COPY OF YOUR MEDICAL RECORD: You have the right to inspect and obtain a copy of the medical records that the Hospital uses to make decisions about you and your treatment. This information includes your medical and billing records, but may not include some mental health information. If you request a copy of your records, we may charge a fee for the cost of providing your records to you.

* “You” in our Notice means a Hospital patient or the personal representative of that patient. A personal representative is any person authorized to act on behalf of the patient with respect to his or her health care. For example, a personal representative may include the parent or guardian of a minor (unless the minor has the authority under California law to act on their own behalf), the guardian or conservator of an adult patient, or the person authorized to act on behalf of a deceased patient.
**Right to an Accounting of Hospital Disclosures of Your Medical Information:** You have the right to request an “accounting of disclosures” which is a list describing how we have shared your medical information with outside parties. This accounting is a list of the disclosures we made after April 14, 2003 of your medical information for purposes other than treatment, payment and health care operations, as those functions are described below.

**Right to Add an Addendum or Correct Your Medical Record:**
- **Addendum:** An adult patient of the Hospital who believes that an item or statement in his/her medical record is incorrect or incomplete has the right to provide the Hospital with a written addendum to his/her record.
- **Correction:** If you believe that medical information the Hospital has on file about you is incorrect or incomplete, you may ask us to correct the medical information in your records. The Hospital can only correct information that we created or that was created on our behalf. If your medical information is accurate and complete, we may deny your request. If we deny any part of your request, we will provide you a written explanation of our reasons.

**Right to Request Restrictions:** You have the right to request restrictions on certain uses or disclosure of your medical information. For example, you may request that your name not appear in the Hospital’s Patient Directory while you are here as an inpatient. Requests for restrictions must be in writing; the appropriate instructions and forms are available at registration areas and on our Internet sites (http://www.lpch.org or http://www.stanfordhospital.com). We are not required to agree to your requested restriction. However, if we do agree, we will comply with your request unless the information is needed to provide you emergency treatment or comply with the law. If we cannot accept your request, we will explain to you in writing why we cannot do so.

**Right to Request Confidential Communications:** You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. You may request confidential communications during your registration process at the Hospital. We will not ask you the reason for your request, and we will try to accommodate all reasonable requests.

**Right to a Copy of This Notice Upon Request:** You have the right to a copy of this notice. It is available in registration areas and on our Internet sites (http://www.lpch.org or http://www.stanfordhospital.com) in the Patient & Visitors section under Patient Services.

**Contact Information:** To obtain information about how to request a copy of your medical records, receive an accounting of disclosures of, or correct or add an addendum to your medical information:

- **SHC Patients**  
  Phone: (650) 723-5721  
  Web: http://www.stanfordhospital.com
  and look in the “Patients & Visitors” section under “Patient Services”

- **LPCH Patients**  
  Phone: (650) 497-8334  
  Web: http://www.lpch.org  
  and look in the “Patients & Visitors” section under “Patient Services”

To obtain information on requesting a copy of your billing records call (800) 333-7491.
The following sections describe different ways that we use and disclose your medical information. For each category of uses or disclosures we will provide examples. To respect your privacy, we will try to limit the amount of information that we use or disclose to that which is the “minimum necessary” to accomplish the purpose of the use or disclosure. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

**FOR TREATMENT:** We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, residents, nurses, technicians, medical students, or other Hospital personnel who are involved in your care at the Hospital. For example, a doctor treating you for a broken leg needs to know if you have diabetes because diabetes can slow the healing process. In addition, the doctor may need to tell the Hospital dietitian if you have diabetes so that we can arrange for appropriate meals. Different departments of the Hospital also may share medical information about you in order to coordinate the different services you need, such as pharmacy, lab work and x-rays.

**FOR PAYMENT:** We may use and disclose medical information about you to bill and receive payment for the treatment and services you receive. For example, we may need to give your health plan information about a surgery you received at the Hospital so your health plan will pay us or reimburse you for the surgery. We may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment. Special authorization is needed to release medical information about you for payment purposes if you receive certain types of services, including those related to substance abuse, mental health or tests related to HIV.

**FOR HEALTH CARE OPERATIONS:** We may use and disclose medical information about you for functions that are necessary to run the Hospital and assure that all of our patients receive quality care. We may also share your medical information with affiliated health care providers so that they may jointly perform certain business operations along with the Hospital. For example, we may use medical information to review our treatment and services and evaluate the performance of our staff in caring for you. We may combine medical information about many of our patients to decide what additional services the Hospital should offer, what services are not needed, and whether certain new treatments are effective. We may share information with doctors, residents, nurses, technicians, medical students, and other personnel for quality assurance and educational purposes. We may also compare the medical information we have with information from other hospitals to see where we can make improvements in the care and services we offer.

**BUSINESS ASSOCIATES:** The Hospital contracts with outside companies that perform business services for us, such as billing companies, management consultants, quality assurance reviewers, accountants or attorneys. In certain circumstances, we may need to share your medical information with a business associate so it can perform a service on our behalf. The Hospital will limit the disclosure of your information to a business associate to the amount of information that is the “minimum necessary” for the company to perform services for the Hospital. In addition, we will have a written contract in place with the business associate requiring it to protect the privacy of your medical information.

**APPOINTMENT REMINDERS:** We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at the Hospital.

**TREATMENT ALTERNATIVES:** We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.

**HEALTH-RELATED BENEFITS AND SERVICES:** We may use and disclose medical information to tell you about health-related benefits or services that may be of interest to you.

**HOSPITAL PATIENT DIRECTORY:** We include limited information about you in the Hospital’s Patient Directory, while you are receiving care as an inpatient. This information includes only your name, room and phone number in the Hospital. We make this information available so that individuals can contact or visit you in the
Hospital. Unless you specifically request that your information be excluded from the Patient Directory, we may release this directory information to people who ask for you by name.

**INDIVIDUALS INVOLVED IN YOUR CARE:** If your family or friends ask for information about you, we may tell them that you are in the Hospital and describe your general condition. This does not apply to patients who are receiving treatment for certain conditions, such as mental health or substance/alcohol abuse. If there are individuals to whom we should not disclose information, you need to let us know this in a written request. In addition, we may disclose medical information about you to an organization assisting in a disaster relief effort (such as the Red Cross) so that your family can be notified about your condition, status and location.

**RELIGIOUS AFFILIATION:** We provide information about your religious affiliation to members of the clergy employed in our Spiritual Care Services Office, unless you specifically request that we not do so.

**FUNDRAISING ACTIVITIES:** We may provide your date of admission and basic contact information (no medical information is provided) to the Lucile Packard Foundation for Children’s Health or the Stanford University Office of Medical Development for purposes of conducting fundraising on the Hospitals’ behalf. These organizations may contact you in an effort to raise money for the Hospital and its operations. If you receive a request for donations from either organization, it will include information indicating how you can opt out from receiving any future requests.

**RESEARCH:** As academic medical centers, both SHC and LPCH have active research programs that conduct studies that may involve your current care or that involve reviews of your medical history. For example, a study may involve an investigational procedure to treat a condition or compare the health and recovery of patients who have received one medication to those who have received another, for the same condition. We generally ask for your written authorization before using your medical information or sharing it with others in order to conduct research. Under limited circumstances we may use and disclose your medical information without your authorization. In most of these latter situations, we must obtain approval through an independent review process to ensure that research conducted without your authorization poses minimal risk to your privacy.

**TO PREVENT A SERIOUS THREAT TO HEALTH OR SAFETY:** We may use and disclose certain information about you when necessary to prevent a serious threat to your health and safety or the health and safety of others. However, any such disclosure will only be to someone able to help prevent the threat, such as law enforcement, or to a potential victim. For example, we may need to disclose information to police when a patient reveals that he/she has participated in a violent crime.

**SPECIAL SITUATIONS THAT DO NOT REQUIRE US TO OBTAIN YOUR AUTHORIZATION**

**WORKERS’ COMPENSATION:** We may release medical information about you for workers’ compensation or similar programs. These programs provide benefits for work-related injuries or illness.

**PUBLIC HEALTH ACTIVITIES:** We may disclose medical information about you for public health activities. These activities include, but are not limited to the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report the abuse or neglect of children, elders and dependent adults;
- to report reactions to medications or problems with products;
- to notify you of the recall of products you may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe you have been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law;
• to report all inpatient admissions, emergency department visits and same-day-surgeries to California’s Office of Statewide Health Planning and Development; and
• to notify appropriate state registries, such as the Northern California Cancer Center or the California Emergency Medical Services Authority, when you seek treatment at the Hospital for a reportable condition.

**Health Oversight Activities:** We may disclose medical information to a health care oversight agency, such as the California Department of Health and Human Services or the Joint Commission on Accreditation of Healthcare Organizations, for activities authorized by law. These oversight activities include audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

**Lawsuits and Disputes:** If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute.

**Law Enforcement:** We may release medical information if asked to do so by law enforcement officials in the following limited circumstances:

- In response to a court order, subpoena, warrant, summons or similar process;
- To identify or locate a suspect, fugitive, material witness, or missing person;
- About the victim of a crime if, under certain limited circumstances, we are unable to obtain the person’s agreement;
- About a death we believe may be the result of criminal conduct;
- About criminal conduct at the Hospital; and
- In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

**Coroners, Medical Examiners and Funeral Directors:** We may release medical information to a coroner or medical examiner. This may be necessary to identify a deceased person or determine the cause of death. We may also release medical information about patients of the Hospital to funeral directors as necessary to carry out their duties with respect to the deceased.

**Organ and Tissue Donation:** If you are a potential organ donor, we may release medical information to organizations that handle organ, eye, or tissue procurement or transplantation. The procurement or transplantation organization needs you to authorize any actual donations.

**Military and Veterans:** If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

**National Security and Intelligence Activities:** Upon receipt of a proper request, we may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

**Inmates:** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release may be necessary for the institution to provide you with health care; to protect your health and safety or the health and safety of others; or for the safety and security of the correctional institution.

**Other Uses or Disclosures Required By Law:** We will also disclose medical information about you when required to do so by federal, state or local laws that are not specifically mentioned in this notice.

Results of Convergent Validity Workgroups March 2003

29
We reserve the right to change our privacy practices and update this notice accordingly. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We post copies of the current notice in the Hospital and on our Internet sites (http://www.lpch.org or http://www.stanfordhospital.com) in the Patient & Visitors section under Patient Services. If the notice is changed, we will ask you to acknowledge receipt of the new notice the next time you seek care at the Hospital after the new effective date. The notice contains the effective date on the first page, in the top right-hand corner.

**COMPLAINTS**

If you believe your privacy rights have been violated, you may file a complaint with the Hospital or with the Secretary of the Department of Health and Human Services (200 Independence Avenue, S.W., Washington, D.C. 20201). To file a complaint with the Hospital, contact:

**SHC Patients**
Community and Patient Relations
300 Pasteur Drive, H1401
Stanford, CA 94305
Phone: (650) 723-7167
Fax: (650) 725-8907

**LPCH Patients**
Patient Relations
725 Welch Road
Palo Alto, CA 94304
Phone: (650) 498-4847
Fax: (650)

No one will retaliate or take action against you for filing a complaint.

**OTHER USES OF MEDICAL INFORMATION**

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written authorization. If you provide us authorization to use or disclose medical information about you, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose medical information about you for the activities covered by the authorization. You understand that we are unable to take back any disclosures we have already made with your authorization, and that we are required to retain our records of the care that we provided to you.

**IF YOU HAVE ANY QUESTIONS ABOUT THIS NOTICE PLEASE CONTACT THE HOSPITAL’S PRIVACY OFFICER @ (650) 725-6291**
Summary NOTICE OF PRIVACY PRACTICES

THIS IS A SUMMARY OF OUR NOTICE OF PRIVACY PRACTICES, WHICH DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. WE HAVE ALSO PROVIDED YOU WITH A FULL VERSION OF THE NOTICE.

Our Pledge to Protect your Privacy:
Stanford Hospital and Clinics (SHC) is committed to protecting the privacy of your medical information. Your care and treatment is recorded in a medical record. So that we can best meet your medical needs, we share your medical record with all the health care providers involved in your care. Only to the extent necessary, we share your information to conduct our business operations, to collect payment for the services we provide to you and to comply with the laws that govern health care. We will not use or disclose your information for any other purpose without your permission.

You have the following rights regarding your medical information:
º to inspect and obtain a copy of your medical records, subject to some special requirements for mental health data;
º to request restrictions on certain uses or disclosures of your medical information;
º to request an accounting of SHC’s disclosures of your medical information;
º to add an addendum to or correct your medical record;
º to request that we communicate with you in a certain way or at a certain location; and
º to receive a copy of a full version of our Notice of Privacy Practices.

How we may use and disclose medical information about you:
º to provide you with medical treatment and services;
º to bill and receive payment for the treatment and services you receive;
º for functions necessary to run SHC and assure that our patients receive quality care;
º to provide basic contact information to our development office for purposes of fundraising for SHC (none of your medical information will be provided to the development office);
º to support our research mission as an academic medical center (we generally ask for your authorization before using your medical information to conduct research); and
º as required or permitted by law.

There are special situations where we may disclose medical information about you without your authorization, such as:
º for workers’ compensation or similar programs;
º for public health activities (e.g., reporting abuse or adverse reactions to medications);
º to a health care oversight agency, such as the California Department of Health Services;
º in response to a court or administrative order, subpoena, warrant or similar process;
º to law enforcement officials in certain limited circumstances;
º to a coroner, medical examiner or funeral director; and
º for organ procurement or transplantation, if you are a potential donor.

We reserve the right to change our privacy practices and update this notice. Please see our full Notice of Privacy Practices for a more detailed description of our privacy practices, your rights regarding your medical information and pertinent contact information.

For further information about the full Notice, please contact SHC’s Privacy Officer at (650) 725-6291.
Summary NOTICE OF PRIVACY PRACTICES

THIS IS A SUMMARY OF OUR NOTICE OF PRIVACY PRACTICES, WHICH DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. WE HAVE ALSO PROVIDED YOU WITH A FULL VERSION OF THE NOTICE.

Our Pledge to Protect your Privacy:

Lucile Packard Children’s Hospital (LPCH) is committed to protecting the privacy of your or your child’s medical information. Your or your child’s care and treatment is recorded in a medical record. So that we can best meet your or your child’s medical needs, we share that medical record with all the health care providers involved in your or your child’s care. Only to the extent necessary, we share your or your child’s information to conduct our business operations, to collect payment for the services we provide and to comply with the laws that govern health care. We will not use or disclose your or your child’s information for any other purpose without your permission.

You have the following rights regarding you or your child’s medical information:

º to inspect and obtain a copy of your medical records, subject to some special requirements for mental health data;
º to request an accounting of LPCH’s disclosures of your medical information;
º to add an addendum to or correct your medical record;
º to request restrictions on certain uses or disclosures of your medical information;
º to request that we communicate with you in a certain way or at a certain location; and
º to receive a copy of a full version of our Notice of Privacy Practices.

How we may use and disclose medical information about you or your child:

º to provide you with medical treatment and services;
º to bill and receive payment for the treatment and services you receive;
º for functions necessary to run LPCH and assure that our patients receive quality care;
º to provide basic contact information to our development office for purposes of fundraising for LPCH; (no medical information is provided);
º to support our research mission as an academic medical center; (we generally ask for your authorization before using your medical information to conduct research); and
º as required or permitted by law.

There are special situations where we may disclose medical information about you or your child without your authorization, such as:

º for public health activities (e.g., reporting abuse or reactions to medications);
º to a health care oversight agency, such as the California Department of Health Services;
º in response to a court or administrative order, subpoena, warrant or similar process;
º to law enforcement officials in certain limited circumstances;
º to a coroner, medical examiner or funeral director; and
º for organ procurement or transplantation, if you are a potential donor.

We reserve the right to change our privacy practices and update this notice. Please see our full Notice of Privacy Practices for a more detailed description of our privacy practices, your rights regarding you or your child’s medical information and pertinent contact information.

For further information about the full Notice, please contact LPCH’s Privacy Officer @ (650) 725-6291.
NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

[This Notice describes our institution’s practices---state designations (OHCA, single 'affiliated' covered entity)—list entities included in designation—all entities listed are required to abide by the terms of this Notice…]

We understand that medical information about you and your health is personal. This Notice provides you with what you should know about:

I. Your health record and reasons why information in your record may be used
II. Your health information rights
III. How the information in your record may be used
IV. Our duties to protect your health information
V. Other important information

The section below titled “Understanding your Health Record/Information” describes the information that may be in your record and lists the reasons why your information may be used. You can get information about how your information may be used for each item listed in this section, by turning to the page and section that is listed next to each item.

I. Understanding your Health Record/Information

Each time you visit a hospital, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment. This information, often referred to as your health or medical record, not only serves as a legal document describing the care you received but serves as a:
Basis for planning your care and treatment
See page 5 under “How we may use or disclose your information for treatment”

Means of communication among the many health professionals who contribute to your care
See page 5 under “How we may use or disclose your information for treatment”

Means by which you or a third-party payer can verify that services billed were actually provided
See page 5 under “How we may use or disclose your information for payment”

A tool in educating health professionals
See page 6 under “How we may use or disclose your information for health care operations”

A source of data for business development needs
See page 6 under “How we may use or disclose your information for health care operations”

A tool with which we can assess and continually work to improve the care we render and the outcomes we achieve
See page 6 under “How we may use or disclose your information for health care operations”

A source of data for medical research (with your permission or as permitted by law)
See page 6 under “Research”

A source of information for public health officials charged with improving the health of the nation
See page 7 under “Public health”

Understanding what is in your record and how your health information is used helps you to:

ensure its accuracy

better understand who, what, when, where, and why others may access your health information

make more informed decisions when authorizing disclosure to others
II. Your Health Information Rights

Although your health record is the physical property of the healthcare practitioner or facility that compiled it, the information belongs to you. You have the following rights regarding medical information we maintain about you:

Right of access to inspect and copy
• You have the right to inspect and copy health information in your medical and billing record with the exception of items prohibited by law. To request access to inspect and copy health information in your medical and billing record, you must submit your request in writing to the appropriate department/address indicated in the “Contact Information” section below. If you request a copy of your health information, a fee for the costs of copying may apply. In limited circumstances, we may deny your request to inspect and copy your health information. If you are denied access to health information, in some instances you may request that the denial be reviewed. An independent review will be conducted. We will comply with the outcome of the review.

Right to request an amendment to your record

You have the right to request an amendment to your record if you feel that medical information we have about you is incorrect or incomplete. You have the right to request an amendment for as long as the information is kept by or for the hospital. To request an amendment, you must submit your request in writing to the appropriate department/address indicated in the “Contact Information” section below. In addition, you must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

• Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
• Is not part of the medical information kept by or for the hospital;
• Is not part of the information which you would be permitted to inspect and copy; or
• Is accurate and complete

Even if we deny your request for amendment, you have the right to submit a written addendum, not to exceed 250 words, with respect to any item or statement in your record you believe is incomplete or incorrect. If you clearly indicate in writing that you want the addendum to be made part of your medical record we will attach it to your records and include it whenever we make a disclosure of the item or statement you believe to be incomplete or incorrect.

Right to an Accounting of Disclosures
• You have the right to request a list (called an accounting of disclosures) of certain disclosures we made about you. Only those disclosures that must be listed as provided by law will appear on the accounting of
disclosures list. The items that typically would be listed on an accounting of disclosures list are indicated throughout the section titled “How We May Use and Disclose Health Information About You”. To request an accounting of disclosures, you must submit your request to the department/address indicated in the “Contact Information” section below.

Right to Request Restrictions

- **YOU HAVE THE RIGHT TO REQUEST A RESTRICTION ON CERTAIN USES AND DISCLOSURES OF YOUR INFORMATION FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS. YOU ALSO HAVE THE RIGHT TO REQUEST A LIMIT ON THE MEDICAL INFORMATION WE DISCLOSE ABOUT YOU TO SOMEONE WHO IS INVOLVED IN YOUR CARE OR THE PAYMENT FOR YOUR CARE, LIKE A FAMILY MEMBER OR FRIEND. FOR EXAMPLE, YOU CAN REQUEST THAT WE NOT DISCLOSE INFORMATION ABOUT A PROCEDURE THAT YOU HAD. WE ARE NOT REQUIRED TO AGREE TO YOUR REQUEST. IF WE DO AGREE, WE WILL COMPLY WITH YOUR REQUEST UNLESS THE INFORMATION IS NEEDED TO PROVIDE YOU EMERGENCY TREATMENT OR AS IS OTHERWISE REQUIRED BY LAW. YOU CAN SPEAK DIRECTLY WITH YOUR HEALTH CARE PROVIDER CONCERNING YOUR REQUEST FOR THESE TYPES OF RESTRICTIONS.**

- **YOU HAVE THE RIGHT TO REQUEST A RESTRICTION ON THE USE AND DISCLOSURE OF YOUR HEALTH INFORMATION FOR THE FACILITY DIRECTORY. WHEN YOU ARE AN INPATIENT IN OUR HOSPITAL, THE FACILITY DIRECTORY LISTS YOUR NAME, YOUR ROOM NUMBER, GENERAL CONDITION AND IF YOU TELL US, YOUR RELIGIOUS AFFILIATION. THE INFORMATION LISTED IN THE FACILITY DIRECTORY IS AVAILABLE TO ANYONE THAT ASKS FOR YOU BY NAME. YOU CAN REQUEST A RESTRICTION ON THE USE AND DISCLOSURE OF YOUR HEALTH INFORMATION FOR THE FACILITY DIRECTORY BY “OPTING OUT” OR REQUESTING THAT WE DO NOT INCLUDE ANY OR ALL OF YOUR INFORMATION IN THE FACILITY DIRECTORY. TO “OPT OUT” OF THE FACILITY DIRECTORY, YOU MUST MAKE YOUR REQUEST IN WRITING THROUGH THE ADMITTING OR REGISTRATION DESK.**

Right to Confidential Communications

- **You have the right to request communications of your health information by alternative means or at alternative locations. For example, you can request that we only contact you at work or by mail. We will accommodate all reasonable requests. You must submit your written request for confidential communications directly to your health care provider.**

Right to Notice

- **You have the right to adequate notice of how we use and disclose your health information. The Notice (or Notice of Privacy Practices) must also advise you of your rights and our legal duties with respect to your health information. You have the right to receive a paper copy of the Notice upon request. A copy of the Notice currently in effect will be available through your health care provider.**
III. How We May Use and Disclose Health Information About You

We can only disclose information in your record 1) with your permission or 2) if federal, state or local law tells us that we can or must disclose information in your record. If a federal, state or local law tells us that we can or must disclose information in your record, in certain cases, we will list the people who received your information in a report to you if you ask. Page 4, under the section titled “Right to an Accounting of Disclosures” explains how you can request a list of the people who received your information. The disclosures described below that will typically be listed on an Accounting of Disclosures are noted with the statement “Included in an Accounting for Disclosures”.

We will not use or disclose your health information without your authorization, except as described in this notice.

1) How we may use or disclose your health information for treatment.

For example: We may use or disclose medical information about you to doctors, nurses, technicians, medical students, or other hospital personnel who are involved in taking care of you at the hospital or medical clinic. Information obtained by a nurse, physician, or other member of your healthcare team will be recorded in your record and used to determine the course of treatment that should work best for you. Your physician will document in your record his or her expectations of the members of your healthcare team. Members of your healthcare team will then record the actions they took and their observations. In that way, the physician will know how you are responding to treatment.

We will also provide your physician or a subsequent healthcare provider with copies of various reports that should assist him or her in treating you once you are discharged from the hospital or upon completion of your course of treatment.

2) How we may use or disclose your health information for payment.

For example: We may use or disclose medical information about you so that the treatment and services you receive at the hospital may be billed to and payment may be collected from you, an insurance company or a third party. For example, we may need to give your health plan information about surgery you received at the hospital so your health plan will pay us or reimburse you for the surgery. We may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment.
3) How we may use or disclose your health information for health care operations.

For example: Members of the medical staff, the risk or quality improvement manager, or members of the quality improvement team may use information in your health record to assess the care and outcomes in your case and others like it. This information will then be used in an effort to continually improve the quality and effectiveness of the health care and service we provide. We may also use or disclose information to doctors, nurses, technicians, medical students, and other hospital personnel for review and learning purposes.

4) How we may use or disclose your health information for purposes other than treatment, payment and health care operations

Facility Directory

Unless you notify us that you object we will use your name, location in the facility, general condition, and religious affiliation for directory purposes. This information may be provided to members of the clergy and, except for religious affiliation, to other people who ask for you by name. See page 4 under “Right to Request Restrictions” for information on what to do if you object to your information being in the facility directory.

Notification:

We may use or disclose information to notify or assist in notifying a family member, personal representative, or another person responsible for your care, your location and general condition.

Communication with family:

Health professionals, using their best judgement, may disclose to a family member, other relative, close personal friend or any other person you identify, health information relevant to that person’s involvement in your care or payment related to your care.

Research:

We may use or disclose information to researchers when their research has been approved by an institutional review board (IRB) that has reviewed the research proposal and established protocols to ensure the privacy of your health information. We may also use or disclose information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave the hospital. We will almost always ask for your specific permission if the researcher will be involved in your care.

Disclosures made outside our institution for an IRB approved research activity are typically Included in an Accounting for Disclosures.

Funeral directors:

We may use or disclose health information to funeral directors consistent with applicable law to carry out their duties. Included in an Accounting for Disclosures
Organ procurement organizations:
Consistent with applicable law, we may disclose health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation and transplant. Included in an Accounting for Disclosures

Appointment Reminders:
We may use or disclose health information to contact you as a reminder that you have an appointment for treatment or medical care at the hospital or medical clinic.

Treatment Alternatives:
We may use or disclose health information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.

Health-Related Products and Services:
We may use and disclose medical information to tell you about our health-related products or services that may be of interest to you.

Customer Service Program: {include specifics here}

Fund raising:
We may contact you as part of a fund-raising effort.

Food and Drug Administration (FDA):
We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement. Included in an Accounting for Disclosures

Workers compensation:
We may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to workers compensation or other similar programs established by law. Included in an Accounting for Disclosures

Public health:
As required by law, we may disclose your health information to public health or legal authorities for activities which include the following:

- To prevent or control disease, injury or disability;
- To report births and deaths;
- To report the abuse or neglect of children, elders and dependent adults;
- To report reactions to medications or problems with products;
- To notify people of recalls of products they may be using;
- To notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- To notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

Disclosures made for public health activities are Included in an Accounting for Disclosures.

Health oversight activities:

Results of Convergent Validity Workgroups March 2003
We may disclose medical information to a health oversight agency for activities authorized by law. Health oversight agencies include the Department of Health Services (DHS) and the Department of Health and Human Services (HHS). Oversight activities include, for example, audits, investigations, inspections and licensure. 

**Included in an Accounting for Disclosures**

**Correctional institution:**

Should you be an inmate of a correctional institution, we may disclose to the institution or agents thereof health information necessary for your health and the health and safety of other individuals.

**Law enforcement:**

We may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena. **Included in an Accounting for Disclosures**

**Lawsuits and Disputes:**

If you are involved in a lawsuit or dispute, we may disclose health information about you in response to a court or administrative order. We may also disclose health information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request (which may include written notice to you) or to obtain an order protecting the information requested. **Included in an Accounting for Disclosures**

**As Required by Law:**

We will disclose medical information about you when required to do so by federal, state or local law. **Included in an Accounting for Disclosures**

**To Avert a Serious Threat to Health or Safety:**

We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat. **Included in an Accounting for Disclosures**

**Other Uses of Medical Information**

**Business associates:**

There are some services provided in our organization through contracts with business associates. An example is a copy service we use when making copies of your health record. When these services are contracted, we may disclose your health information to our business associate so that they can perform the job we've asked them to do and bill you or your third-party payer for services rendered. To protect your health information, however, we require the business associate to appropriately safeguard your information.

**Other uses and disclosures**

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, this will stop any further use or disclosure of your medical information for the purposes covered by your written authorization, except if we have already acted in reliance on your permission. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

**IV. Our Responsibilities**

This organization is required to:
• maintain the privacy of your health information
• provide you with a notice as to our legal duties and privacy practices with respect to information we collect and maintain about you
• abide by the terms of this notice

V. Other Important Information

Changes to this Notice
We reserve the right to change the terms of this notice and to make the new provisions effective for all protected health information we maintain. Should there be a material change to how we use or disclose your health information or to your individual rights or our legal duties, we will mail a revised notice to the address you’ve supplied us. Additionally, a copy of the revised notice will be available at your physician’s office, registration and admitting desks upon request.

For More Information or to Report a Problem
If you believe your privacy rights have been violated, you may file a complaint with the hospital or with the Secretary of the Department of Health and Human Services. To file a complaint with the hospital, contact [insert name, title, and phone number of contact person] All complaints must be submitted in writing. **You will not be penalized for filing a complaint.**

Effective Date: [DATE]
This Notice of Privacy Practices describes how (List entities) may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information.

“Protected health information” is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services. If you have questions about any part of this Notice or if you want more information about the privacy practices at any of the above listed organizations, please contact:

Phone Numbers of Privacy Office(s)

1. OUR DUTIES TO YOU REGARDING PROTECTED HEALTH INFORMATION

The above listed organizations are required by law to (1) make sure that medical information that identifies you is kept private, (2) give you this notice of our legal duties and privacy practices with respect to medical information about you, (3) follow the terms of the notice that is currently in effect, and (4) communicate any changes to the Notice to you.

We reserve the right to change this Notice of Privacy Practices at any time in the future. The Notice’s effective date is found at the top of the first page. We reserve the right to make the revised or changed notice effective for protected health information we already have about you as well as any information we receive in the future. You may request a copy of any revised notice of Privacy Practices by: 1) calling the compliance number above, 2) asking for one at your next visit to our organization, or 3) via our website at . Until such amendment is made, we are required by law to comply with this Notice.

We will also post a copy of the current Notice at certain designated registration areas throughout our hospital and clinics. In addition, upon your first visit to our organization, we will provide you with a summary brochure of this Notice that will include instructions regarding how to obtain a comprehensive copy of this Notice.

2. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

A. Uses and Disclosures of Protected Health Information for Treatment, Payment and Healthcare Operations

The law permits us to use or disclose your protected health information for the following purposes:

1) Treatment. We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services. Doctors and/or residents, nurses, technicians, medical students, or other health care personnel who are involved in taking care of you use medical information about you.

For example, a doctor or resident treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. In addition, the doctor may need to tell the dietitian if you have diabetes so that we can arrange for appropriate meals. Different departments of the hospital and/or clinics also may share protected health information about you in order to coordinate the different things you need, such as prescriptions, lab work and x-rays.

We may also disclose protected health information about you to people outside our organization that will be involved in your medical care or others we use to provide services that are part of your care. For example, your family doctor/primary care physician may want to be informed of your admission to our hospital, the treatment that you received while you were a patient at our hospital, and the result of your treatment so that (s)he may provide the appropriate follow-up care after you are discharged.

2) Payment. Your protected health information will be used or disclosed, as needed, to obtain payment for your health care services. This may include certain activities that we are required to undertake before payment can be obtained from your health insurance plan or other third party. These activities may include determining eligibility or
coverage of benefits, reviewing services provided to you as medically necessary, and obtaining approval for a hospital stay from your health insurance plan.

3) Health Care Operations. We will use or disclose, as needed, protected health information about you in order to support the daily activities of providing health care. These uses and disclosures are necessary to run the hospital and clinics and make sure that all of our patients receive quality care. These activities include, but are not limited to, quality assessment activities, audits, investigations, oversight or staff performance reviews, training of medical students, licensing, and conducting or arranging for other health care related activities.

For example, we may use your protected health information to review our treatment and services and to evaluate the performance of our staff in caring for you. We may also combine protected health information about many hospital patients to decide what additional services the hospital or clinic could offer, what services are not needed, and whether certain new treatments are effective. Since we are a teaching institution, we may also disclose information to doctors, residents, nurses, technicians, students, community physicians, and other hospital or clinic personnel for research studies and learning purposes. We will remove information that identifies you from this set of medical information so others may use it to study medical care and medical care delivery without learning who you are.

Information provided to you:

- Appointment Reminders: We may use and disclose your medical information to contact you as a reminder that you have an appointment for treatment or medical care at the hospital or clinic.
- Treatment Alternatives: We may use and disclose your medical information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.
- Medical-Related Benefits and Services: We may use and disclose your medical information to tell you about medical-related benefits or services that may be of interest to you, such as diabetes management classes, stress management classes, etc.

B. Uses and Disclosures of Protected Health Information Based upon Your Written Authorization

Except as described in this Notice of Privacy Practices, we will not use or disclose your protected health information without your written authorization. If you do authorize us to use or disclose your protected health information for another purpose, you may revoke your authorization in writing at any time.

C. Other Permitted and Required Uses and Disclosures That May Be Made With Your Authorization or Opportunity to Object

We may use and disclose your protected health information in the situations listed below. You have the opportunity to agree or object to the use or disclosure of all or part of your protected health information. If you are not present or able to agree or object to the use or disclosure of the protected health information, then your physician or other clinical staff member involved in your care may, using their professional judgment, determine whether the disclosure is in your best interest. In this case, only the protected health information that is relevant to your health care will be disclosed.

Facility Directories. Unless you object, we may include certain limited information about you in the facility directories while you are a patient. This information may include your name, location in the hospital or clinic, your general medical condition (e.g., fair, stable, etc.) and your religious affiliation. This information, except your religious affiliation, may be provided to people who ask for you by name. Your religious affiliation may be given to a member of the clergy, such as a priest or rabbi, even if they don't ask for you by name. This is so that your family, friends, and clergy can visit you in the hospital and generally know how you are doing. If you do not want us to release this information, tell either your nurse or an admission clerk upon admission to our hospital or clinic.

Others Involved in Your Care. Unless you object, we may disclose your protected health information to notify or assist in notifying a family member, your personal representative or another person responsible for your care about your location, your general condition or in the event of your death. If you are able and available to agree or object, we will give you the opportunity to object prior to making this notification. If you are unable or unavailable to agree or object, our medical professionals will use their best judgment in communication with your family and others involved in your care.

Marketing and Fundraising. We will not use or disclose your protected health information for Marketing or Fundraising purposes until we obtain your written authorization. We do not provide or sell your protected health information to any outside marketing firms or agencies.
We may use certain information (name, address, telephone number, dates of service, age and gender) to contact you in the future to raise money for [List Entities]. We may also provide your name to [Foundation Name] for the purpose of fundraising for these entities. The money raised will be used to expand and improve services and programs we provide the community. If you choose not to have contact you for fundraising efforts, you may opt out of any future telephone calls or mailings by making your request to [information].

D. Other Permitted and Required Uses and Disclosures That May Be Made Without Your Authorization or Opportunity to Object

We may use or disclose your protected health information in the following situations without your authorization. These situations include:

**Required by law.** We may use or disclose your protected health information when required to do so by federal, state or local law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. For example, the Office of Civil Rights or the Office of the Inspector General may require access to your protected health information while conducting audits or investigations of reported privacy breaches or violations. By law, we must make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of the Health Insurance Portability and Accountability Act of 1996.

**Public Health and Safety.** As required by law, we may disclose your protected health information to public health authorities for purposes related to: 1) preventing or controlling disease, injury or disability; 2) reporting births and deaths; 3) reporting child abuse or neglect; 4) reporting domestic violence; 5) reporting to the Food and Drug Administration problems with products and reactions to medications; 6) notifying people of recalls of products they may be using; and 7) reporting disease or infection exposure to a person who may have been exposed or may be at risk for contracting or spreading a disease or condition. We may also disclose your protected health information to appropriate persons in order to prevent or lessen a serious and imminent threat to your health or safety, or the health or safety of another person or the general public. Any disclosure, however, would only be to someone able to help prevent the threat.

**Military Activity and National Security.** When the appropriate conditions apply, we may use or disclose protected health information of individuals who are Armed Forces personnel or veterans (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military service. We may also disclose your protected health information to authorized federal officials for conducting national security and intelligence activities including for the provision of protective services to the President or others legally authorized.

**Health Oversight Activities.** We may disclose your protected health information to authorized federal officials for conducting national security and intelligence activities including for the provision of protective services to the President or others legally authorized.

**Legal Proceedings.** If you are involved in a lawsuit or a dispute, we may disclose your protected health information in response to a court or administrative order. We may also disclose your protected health information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

**Law Enforcement.** We may disclose your protected health information to law enforcement officials for purposes or in situations such as:
- identifying or locating a suspect, fugitive, material witness or missing person;
- in response to a court order, subpoena, warrant, summons or similar process;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person’s agreement;
- about a death we believe may be the result of criminal conduct;
- about criminal conduct at the hospital; and
- in emergency circumstances to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

**Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may disclose your protected health information to the correctional institution or law enforcement official. This disclosure would be necessary (1) for the institution to provide you with medical care; (2) to protect your medical and safety or the medical and safety of others; or (3) for the safety and security of the correctional institution.
Coroners, Funeral Directors, and Organ Donation. We may disclose protected health information to coroners or medical examiners for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose protected health information to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties of making funeral arrangements. If you are an organ or tissue donor, we may disclose protected health information to organizations involved in procuring, banking or transplanting organs and tissues in order to facilitate the donation and transplantation.

Research. We may disclose your protected health information to researchers conducting research that has been approved by an Institutional Review Board, which has reviewed the research proposal and established protocols to ensure the privacy of your protected health information. For example, a research project may involve comparing the medical treatment and recovery of all patients who received one medication to those who received another type of medication for the same condition. All research projects, however, are subject to a special approval process called an Institutional Review Board or Privacy Board. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with the patients’ need for privacy of their medical information. Before we use or disclose protected health information for research, the project will have been approved through this research approval process, but we may disclose protected health information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave the facility, and so long as the information sought is necessary for the research purpose. We will ask for your specific permission if the research involves treatment. If you are asked for such permission, you have the right to refuse.

Worker’s compensation. We may use and disclose your protected health information as necessary to comply with worker’s compensation laws regarding work-related injuries or illness.

Change of Ownership. In the event that (List Entities), is sold or merged with another organization, your medical information/record will become the property of the new owner.

3. YOUR RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU

You have the right to inspect and copy your protected health information. This means you may inspect and obtain a copy of protected health information about you that is contained in a designated record set for as long as we maintain the protected health information. A “designated record set” contains medical and billing records and any other records that your physician or hospital use for making treatment decisions about you, except for psychotherapy notes.

To request a copy of your hospital medical information, contact ___________________________.

To request a copy of your physician or outpatient medical information, contact ___________________________.

You have the right to request restrictions or limitations on certain uses and disclosures of your protected health information. This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment or healthcare operations. You may also request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. In your request, you must tell us (1) what information you want restricted, (2) whether you want to restrict our use, disclosure or both, (3) to whom you want the restriction to apply, for example, disclosures to your spouse, and (4) an expiration date.

We are not required to agree to a restriction that you may request. If the health care provider believes it is in your best interest to permit use and disclosure of your protected health information, then it will not be restricted. If your health care provider does agree to the requested restriction, we may not use or disclose your protected health information in violation of that restriction unless it is needed to provide emergency treatment. With this in mind, please discuss any restriction you wish to request with your physician.
To request a restriction of your hospital information, please send your written request to ______________.

To request a restriction of your outpatient information, please send your written request to ______________.

You have the right to request to receive confidential communications from us by reasonable alternative means or at an alternative location. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.

To request confidential communications of your hospital information, contact ______________.

To request confidential communications of your physician or outpatient medical information, contact ______________.

You have a right to request that we amend your protected health information that is in your designated record set. A “designated record set” contains medical and billing records and any other records that your physician or health care provider use for making treatment decisions about you, except for psychotherapy notes. We will consider your request and will make amendments based on the medical opinion of the health care provider who originated the entry. However, if the health care provider believes the entry should not be amended, we are not required to make the amendment. We will inform you about the denial and how you can disagree with the denial.

For more information about requesting amendments to your hospital designated record set, contact ______________.

For more information about requesting amendments to your outpatient designated record set, contact ______________.

You have a right to receive an accounting of certain disclosures we have made of your protected health information. This right applies to disclosures for purposes other than treatment, payment or health care operations. Nor does this right apply to information provided to you, facility directory listings, and certain government functions as addressed in this Notice of Privacy Practices.

To request an accounting of hospital disclosures, contact the Health Information Management Department, of the hospital.

To request an accounting of outpatient disclosures, contact the Health Information Management Department, of the outpatient clinic.

You have a right to obtain a paper copy of this Notice of Privacy Practices. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice. You may obtain a copy of this Notice on our website at _____ or by contacting _____.

4. CONTACT INFORMATION AND COMPLAINTS

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about access to your medical information or in response to a request you made to amend or restrict the use or disclosure of your medical information or to have us communicate with you in confidence by alternative means or at an alternative location, you may complain to us using the contact information listed at the end of this notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.
We support your right to protect the privacy of your medical information. You will not be penalized for filing a complaint. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Concerns about this Notice of Privacy Practices or how your protected health information is used or disclosed should be directed to any of the contacts listed below:

List numbers of privacy officers.

5. OTHER USES OF YOUR PROTECTED HEALTH INFORMATION

Other uses and disclosures of your protected health information not covered by this Notice or the laws that apply to __________________ will be made only with your written permission. If you provide us with permission to use or disclose your protected health information, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose your protected health information for the reasons covered by your written authorization. We are unable to take back any disclosures we have already made with your permission, and we are required to retain records of the care that we provided to you under that written authorization.