HEALTH INSURANCE PORTABILITY
AND ACCOUNTABILITY ACT

PRIVACY RULE
(HIPAA)

UNIVERSITY OF CALIFORNIA
SYSTEMWIDE STANDARDS
AND IMPLEMENTATION POLICIES
(System Standards)

April 2003
Acknowledgements

The development of the University of California’s HIPAA Standards and Implementation Policies (System Policies) is the result of the collegial effort of committed individuals, hours of intense discussion, lively debate and indepth analysis of both the requirements of the Privacy Rule and the practices of the University of California’s teaching, research and health care mission. Thank you, one and all...

Dr. Charles Mittman, who said on that fateful day in Folsom: “I’ll get us started on the policies” — and he persevered through over 30 versions of what has become affectionately known as “the OPUS”; the HIPAA Legal Team, led by Martha Chase, Anna Orlowski and John Lundberg, who have provided excellent advice and workable interpretations; Dr. Rory Jaffe, our PDA expert who could always find a reference when we demanded it; Rebecca Landes and the IRB Directors, who patiently guided our understanding of the research process; Nancy Capell, who is an editor extraordinaire; Bill Cormier and Chris Norlin, who took a messy draft and made it look professional; those people who made our jobs easier by working harder than ever – Joan Fisher, Marina Lawson, Jean Chao, and Bunny Quartararo; and the Privacy Officers and others from UCOP and each of the academic health centers who signed on early and have endured to make it happen—Jim Herron, Deborah Yano-Fong, Mark Speare, Kevie Naughton, Dr. Gene Spiritus, Marion Mallory, Dr. Alan Robinson, Geneva Harris, Teresa Porter, Patrick Reed, Dr. Mike McCoy, Harry Cordon, Craig Matthews, Elaine Pierce; and Joy Grosser, who provided the quote that sums it up:

“We are wiser because of the collective wisdom.”

It’s been fun…Maria Faer
Contents

I. RESOLUTION OF THE UNIVERSITY OF CALIFORNIA BOARD OF REGENTS ................. 1

II. INTRODUCTION .............................................................................................................. 2

   The Health Insurance Portability and Accountability Act of 1996 (HIPAA) ................ 2

   University of California’s HIPAA Compliance Work-plan ........................................... 2

   HIPAA Privacy Rule ........................................................................................................ 3

      Privacy Principles ........................................................................................................ 3

      Healthcare Provider and Plan Responsibilities .......................................................... 3

      Patient Rights ............................................................................................................. 4

   The Relationship of HIPAA Privacy Protections to California Law ......................... 4

   HIPAA Security Rule .................................................................................................... 5

   Administrative Simplification: Standardization of Transactions ................................ 5

   Purpose, Use And Organization Of The University’s HIPAA Systemwide
   Standards and Implementation Policies ......................................................................... 5

   Organization of the Systemwide HIPAA Policies ....................................................... 6

III. HIPAA PRIVACY RULE STANDARDS ......................................................................... 7

   Standard One: The Organizational Requirements of a Covered Entity .................... 7

      UC Must Designate and Document Covered Entities and Individuals
      Within The Single Health Care Component (SHCC) ................................................. 8

      UC Must Designate a Privacy Official(s) and Individuals Designated
      with the Responsibility for Implementation of the Privacy Rule .............................. 9

      UC Must Establish Policies and Procedures with Respect to the Use and
      Disclosure of PHI ...................................................................................................... 10

      UC Must Train All HIPAA-Covered Workforce Members ..................................... 11

      Standard One: Implementation Policies .................................................................. 12

   Standard Two: Protected Health Information (PHI) and Data Sets ............................ 17
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition of Protected Health Information (PHI)</td>
<td>17</td>
</tr>
<tr>
<td>UC Policies Applying to Campus Activities, Organizations and Students (Section 130)</td>
<td>18</td>
</tr>
<tr>
<td>Employment Records held by the SHCC in its role as employer</td>
<td>19</td>
</tr>
<tr>
<td>Analyzing When an Individual’s Health Information is PHI</td>
<td>19</td>
</tr>
<tr>
<td>Required Disclosures by the SHCC to the UC, the Individual’s Employer</td>
<td>20</td>
</tr>
<tr>
<td>Research Health Information (RHI)</td>
<td>20</td>
</tr>
<tr>
<td>Designated Record Set (DRS)</td>
<td>20</td>
</tr>
<tr>
<td>Exclusions from the DRS</td>
<td>21</td>
</tr>
<tr>
<td>Deidentification of PHI</td>
<td>22</td>
</tr>
<tr>
<td>Limited Data Set and the Data Use Agreement 45 C.F.R. 164.514, 164.528</td>
<td>23</td>
</tr>
<tr>
<td>Date Use Agreement</td>
<td>24</td>
</tr>
<tr>
<td>Standard Two: Implementation Policies</td>
<td>25</td>
</tr>
<tr>
<td>Standard Three: Safeguards for Protected Health Information (PHI)</td>
<td>27</td>
</tr>
<tr>
<td>Institutional Safeguards</td>
<td>27</td>
</tr>
<tr>
<td>Individual Safeguards</td>
<td>27</td>
</tr>
<tr>
<td>Standard Three: Implementation Policies</td>
<td>27</td>
</tr>
<tr>
<td>Standard Four: Required Notice of Privacy Practices and Written Acknowledgment of Receipt</td>
<td>28</td>
</tr>
<tr>
<td>Notice of Privacy Practices (The Notice)</td>
<td>28</td>
</tr>
<tr>
<td>Mental Health Notice</td>
<td>29</td>
</tr>
<tr>
<td>Initial Moment and Signed Acknowledgement</td>
<td>30</td>
</tr>
<tr>
<td>Right to Request Restrictions</td>
<td>30</td>
</tr>
<tr>
<td>Facility Directory 45 C.F.R. 164.510</td>
<td>31</td>
</tr>
<tr>
<td>Personal Representatives</td>
<td>31</td>
</tr>
<tr>
<td>Uses and Disclosures of PHI That Do Not Require Notice and Acknowledgement or Authorization</td>
<td>31</td>
</tr>
<tr>
<td>Standard Four: Implementation Policies</td>
<td>31</td>
</tr>
</tbody>
</table>
Standard Five: Permitted Uses and Disclosures of PHI When the SHCC Provides the Patient with the Notice of Privacy Practices ................................................................. 35

   Permitted Uses and Disclosures that Do Not Require the Individual’s Authorization ................................................................. 35

Minimum Necessary Standard. 45 C.F.R. 164.502 and 164.514 ................................................................. 36

Application of the Minimum Necessary Standard to the Use of PHI for Treatment Purposes.................................................................................................. .......... 37

Incidental Uses and Disclosures................................................................................................ .......... 37

Worker’s Compensation....................................................................................................................... 38

Standard Five Implementation Policies ............................................................................................. 38

Standard Six: Uses and Disclosures of PHI That Require an Authorization from the Individual............................................................................................................ 42

Prior Legal Permissions........................................................................................................ ................ 42

Authorization for Use or Disclosure of Psychotherapy Notes........................................................ 42

Standard Six Implementation Policies........................................................................................... ..... 43

Standard Seven: Uses and Disclosure of PHI to Other Covered and Non-Covered Entities .................................................................................................................. 46

Minimum Necessary Standard.................................................................................................... 46

Treatment Purposes of Another Entity .............................................................................................. 47

Payment Purposes of Another Entity ............................................................................................. .... 47

Operations of Another HIPAA-Covered Entity................................................................................ 47

Other Operations of a Covered Entity........................................................................................... ..... 48

Operations of a Non-HIPAA Covered Entity ................................................................................... 48

Disclosures to a Non-HIPAA Covered Entity for the SHCC’s Teaching Operations ......................... 48

Organized Health Care Arrangement ................................................................................................ 48

Affiliated Covered Entities........................................................................................................ 49

Between Governmental Institutions............................................................................................. 48

Standard Seven: Implementation Policies ........................................................................................ .4 8
Standard Eight: Use and Disclosure Required by Law, Public Health or Judicial and Law Enforcement Proceedings and for Specialized Government Functions. 45 C.F.R. 164.512 ..................................................................................................................... 51

Standard Eight Implementation Policies ................................................................. 53

Standard Nine: Uses And Disclosures For Research ............................................. 53

Impact of HIPAA/The Privacy Rule on Research.................................................... 54

Research-related Health Information (RHI) and the Relationship of Research to the University’s Single Health Care Component (SHCC) .............................................................. 54

Standard Nine Implementation Policies ................................................................. 56

Disclosure of PHI for Research Purposes with the Individual’s Signed Research Authorization ........................................................................................................... 57

Disclosures that Do Not Require Authorization ..................................................... 58

Accounting for Disclosure of PHI for Research Purposes ..................................... 62

Retrospective Research Studies Involving Data Re-analysis ................................... 62

Transition Provision ............................................................................................... 63

Research Database ................................................................................................. 64

Disclosures to Registries ......................................................................................... 64

Clinical Labs that Participate in Research ............................................................. 65

Patient’s Right to Access PHI Created in a Research Trial ................................. 65

Disclosures Related to Adverse Events ................................................................. 65

Redisclosure of PHI by Third Parties ................................................................. 66

Standard Ten: Use and Disclosure of PHI for Institutional Advancement and External Relations .......................................................... 66

Fundraising by the SHCC ..................................................................................... 66

Fundraising Activities that Require the Patient’s Authorization ............................ 66

Marketing by the SHCC ........................................................................................ 66

Marketing Activities that Require the Patient’s Authorization ............................ 66

Two Exceptions to the Required Patient’s Authorization for Marketing .............. 67

SHCC Health Care Communications that are Not Marketing and Do Not Require the Individual’s Authorization ................................................................. 68
Communications with the Media...................................................................................................... 69

Standard Ten: Implementation Policies .......................................................................................... 70

**Standard Eleven: A Patient’s Right to Request Restriction on Uses and**
**Disclosures CFR 164.522........................................................................................................ 74**

Standard Eleven Implementation Policies ..................................................................................... 74

**Standard Twelve: A Patient’s Right To Request Confidential Communications.**
**CFR 164.522......................................................................................................................... 78**

Standard Twelve Implementation Policies ..................................................................................... 81

**Standard Thirteen: A Patient’s Right to Access and Copy the**
**Designated Record Set............................................................................................................. 83**

**Standard Fourteen: The Patient’s Right to an Amendment of the**
**Designated Record Set............................................................................................................. 87**

**Standard Fifteen: Individual’s Right to Request an Accounting of**
**Disclosures of PHI................................................................................................................... 83**

**Standard Sixteen: Permitted Uses and Disclosures to Business Associates (BA). ................. 87**

Identifying Business Associate Relationships ............................................................................. 88

Relationships that are NOT Business Relationships ................................................................. 90

Business Associate Agreement/Amendment Elements ............................................................... 90

SHCC and Business Associate Responsibilities with Respect to Patient Rights ....................... 90

Business Associate Transition Period .......................................................................................... 91

Policy Sixteen Implementation Policies ...................................................................................... 91

**Standard Seventeen: Documentation Requirements............................................................... 93**

APPENDIX A

APPENDIX B
I. RESOLUTION OF THE UNIVERSITY OF CALIFORNIA BOARD OF REGENTS

May 2002

Academic Health Center Health Insurance Portability And Accountability Act (HIPAA) Compliance Program

The University’s individual and institutional providers of health care recognize and respect a patient’s expectations that the privacy and security of individual health information will be protected. The University is committed to implementing policies and practices that will enable us to reasonably and appropriately protect our patient’s privacy while carrying out our mission of care, service, education and research. Compliance with the mandates of The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and Security Regulations requires a thoughtful balance between the rights of the University’s patients to privacy of their protected health information, the patient’s expectation that quality care will be delivered in a cost-effective and timely manner, and society’s expectation that academic health centers will continue to teach and perform leading edge research.

The Board of Regents recognizes and supports the efforts of the members of the University’s Systemwide Taskforce to Implement a HIPAA Compliance Program that will: provide for compliance by developing privacy and security policies applied to those covered entities of the University; demonstrate a commitment and leadership across the organization to the principles embodied in HIPAA; minimize disruption to the care, research and teaching missions of the University; and, enhance patient confidence in the institutions that serve them.
II. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates significant changes in the legal and regulatory environment governing the provision of health benefits, the delivery of and payment for healthcare services, and the security and confidentiality of individually identifiable, protected health information (PHI) in written, electronic or oral formats. The HIPAA Privacy Rule provides for the privacy of an individual’s health information, with a compliance date of April 2003. The HIPAA Security Rule provides for the security of an individual’s health information when the information is transmitted electronically; the compliance date is April 2005. The HIPAA Administrative Simplification Standards provide for the standardization of transactions and formats used for electronic communication of health care data. In 2002 the President signed legislation allowing for a one-year delay in HIPAA Transactions and Code Sets compliance from October 2002 to October 2003.

University of California’s HIPAA Compliance Work-plan

Since the HIPAA Privacy Rule applies to the use and disclosure of an individual’s protected health information, the University’s academic medical centers took a leadership role in recommending a system-wide approach to prepare for compliance with the requirements of HIPAA. In November 2000, the academic medical center CEOs and School of Medicine Deans from the five academic health center campuses (Davis, Irvine, Los Angeles, San Diego, San Francisco) appointed individuals from each of their respective health sciences centers and the Office of the President (Office of the General Counsel, University Auditor, Clinical Services) to the University’s system-wide HIPAA Taskforce (the HIPAA Taskforce) and charged the group with developing a work-plan for achieving academic health system compliance prior to the HIPAA Privacy Rule prior to the effective date of April 2003.

The HIPAA Taskforce soon determined that HIPAA would not only apply to the five University academic health centers, but would also encompass University health care providers at all University campuses and the University self-funded health plans. Consequently, the HIPAA Taskforce broadened its membership and the scope of its efforts to include individuals representative of covered functions and entities from throughout the University. Since November 2000, the HIPAA Taskforce has grown from a group of approximately 20 members to over 115 members with representation from all University campuses, federal Department of Energy Laboratories, and leadership from the Office of Business and Finance charged with HIPAA compliance by the University’s covered self-funded health plans. Appendix A provides a list of those individuals participating in the work of the HIPAA Taskforce as of April 14, 2003.

In May 2002, the University’s Board of Regents took action to support the recommendation of the HIPAA Taskforce that, for purposes of compliance with HIPAA, all University HIPAA-covered entities would comprise a Single Health Care Component (SHCC) and would implement a system-wide approach to achieving compliance with HIPAA. The Privacy Rule requires the University to designate and document the entities and individuals within the University that are a part of the SHCC and, as such, must comply with HIPAA. Further, the University must define those entities and workforce members who are not covered by HIPAA and are not part of the SHCC and
safeguard the flow of protected health care information between the SHCC and non-covered entities and workforce members.

In order to provide for system compliance as a SHCC, the HIPAA Taskforce, in coordination with individuals from throughout the University system, has developed policies, procedures, HIPAA education modules designed to train the workforce on those policies and procedures, and other materials necessary to implement a single system approach to compliance. Appendix B provides a list of University prepared and copyrighted materials included in the University’s HIPAA Implementation Packet. Copies of all materials are available from the University’s Privacy Official or on the University’s HIPAA website at www.universityofcalifornia.edu/hipaa.

The purpose of the University of California’s Systemwide HIPAA Standards and Implementation Policies (System Standards) is to provide uniform compliance standards and implementation policies for all covered entities within the University.

**HIPAA Privacy Rule**

As of April 2003, health care providers, health plans and health care clearinghouses must be in compliance with The Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule). The HIPAA Privacy Rule provides the first comprehensive federal protection for the privacy of health information.

**PRIVACY PRINCIPLES**

The Privacy Rule creates standards that protect a patient or member’s medical records and personal health information and:

1. Gives patients and plan members more control over their health information;
2. Sets boundaries on the use and release of health records;
3. Establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information;
4. Holds violators accountable and imposes civil and criminal penalties for violation of a patient’s privacy rights;
5. Strikes a balance when public responsibility requires disclosure of some forms of data (for example, to protect public health); and
6. Establishes a “federal floor” of safeguards. (State laws with stronger privacy protections take precedence over and above the HIPAA Privacy Rule.)

**HEALTHCARE PROVIDER AND PLAN RESPONSIBILITIES**

In general, the Privacy Rule requires covered entities to:

1. Provide information to patients or plan members about their privacy rights and how their information can be used;
2. Adopt clear privacy policies and procedures;

3. Educate all employees regarding privacy policies and procedures;

4. Designate a Privacy Official or individual to be responsible for seeing that privacy procedures are adopted and followed and/or a HIPAA Office responsible for receiving and handling complaints;

5. Respond to patient or plan members’ requests regarding certain rights provided in the Privacy Rule; and

6. Secure patient and members’ records so that they are available only to those who need them.

**PATIENT RIGHTS**

The Privacy Rule entitles patients or members to:

1. Receive Notice of a HIPAA-covered entity’s practices governing permitted uses and disclosures of PHI;

2. Authorize release and disclosure of PHI as required in the Privacy Rule;

3. Inspect and/or copy PHI;

4. Request that PHI be amended or appended (if information is incorrect or incomplete);

5. Request and receive an accounting of uses and disclosures of PHI, with certain exceptions;

6. Request additional restrictions on use/disclosure of PHI; and

7. Request confidential communications of PHI.

---

**The Relationship of HIPAA Privacy Protections to California Law**

California state laws that address medical confidentiality and access to medical information include: the *Confidentiality of Medical Information Act* which requires patient authorization for release of information unless release is otherwise permitted or required by law; the *Lanterman-Petris-Short Act* that protects mental health information; HIV test confidentiality laws that provide protection for information concerning HIV tests; and the *Information Practices Act*.

HIPAA provides that “…any provision, requirement, standard or implementation specifications of HIPAA shall supersede any contrary provision of State law” for all components of HIPAA, not only those relating to privacy. With few exceptions, when the state law is more protective of privacy rights than the federal law, the state law prevails.

The determination of when state law prevails is complicated by the fact that there has been no historical effort to harmonize state laws relative to medical records or privacy of information. The University’s Office of the General Counsel has been collaborating with others in the state, including the California Healthcare Association (CHA) and California Office of HIPAA
Implementation (CalOHI) to develop a state-wide preemption analysis for all covered entities. To the extent possible, the System Standards provide the University’s required policies and procedures, including where state law provides greater protections for the individual. However, the University and the HIPAA Taskforce recognize that the System Standards is a dynamic document that may require modification as the SHCC implements the policies and procedures and develops best practices.

**HIPAA Security Rule**

The Department of Health and Human Services (DHHS) published the final HIPAA Security Rule on February 20, 2003, with an implementation date of April 2005. The HIPAA Taskforce expects to implement a planning process similar to that used for the Privacy Rule. Moreover, achieving compliance with the Security Rule anticipates that covered entities will build upon the policies and procedures developed for compliance with the Privacy Rule.

**Administrative Simplification: Standardization of Transactions**

Standardization of transactions and formats used for electronic communication of health care data includes: claims or encounter information; health plan eligibility; referral certification and authorization; health care claim status; enrollment and disenrollment; payment and remittance advice; premium payments; and coordination of benefits. Providers do not have to conduct electronic transactions, but providers must comply with the standards if they use electronic transactions. Health plans must use the standards for electronic transactions and accept standard transactions from providers and process them promptly. Covered entities are not permitted to vary the standards. In other words, a health plan and a provider cannot mutually and independently agree to vary the standards. The University has until October 2003 to comply.

**Purpose, Use And Organization Of The University’s HIPAA Systemwide Standards and Implementation Policies**

The University’s Systemwide HIPAA Standards and Implementation Policies (System Standards) provide all covered entities within the SHCC with consistent standards and policies to achieve compliance as a hybrid-covered entity with a Single Health Care Component (SHCC). Individual covered entities and individuals within the SHCC may promulgate more stringent requirements.

The Final Privacy Rule, August 14, 2002, specifically states: “One of the goals in making changes to the Privacy Rule is to simplify, rather than add complexity and to assure that the Privacy Rule does not hamper necessary treatment.” The University supports these principles and has developed the System Standards in order to:

1. Reduce costs of compliance by standardizing the University’s approach and by sharing resources and expertise;
2. Maintain the standards of quality care;
3. Provide scalability and enhance compliance by creating, where appropriate, a single set of policies, procedures and practices;
4. Reduce the University’s business and audit risks by providing consistency of approach, sharing best practices and uniform applications of the “reasonableness and appropriate” principles for HIPAA compliance;

5. Enhance compliance by demonstrating commitment and leadership across the organization and providing support at all levels for the cultural changes necessary to manage privacy and security;

6. Minimize disruption to the care, research, public service and teaching missions of the University;

7. Build patient confidence in and loyalty toward the University;

8. Enhance ability to provide consistency and accountability for documentation and accounting; and

9. Facilitate the transfer of information between the appropriate units within the SHCC.

Organization of the System Standard

The Standard summarizes the University’s legal interpretation of the requirements of the Privacy Rule as applicable to the University. Section III. HIPAA Privacy Rule Standards focuses on the applicability of the Privacy Rule to the SHCC’s health care providers. Section IV. Privacy Rule Requirements for Covered Health Plans: the University as Plan Sponsor, Plan Administrator and the University’s Self-Funded Plans provides the specific Standards and Policies for the University’s self-funded health plans, as well as the requirements of the University as a plan sponsor and plan administrator.

Implementation Policies are the University’s policy interpretations of the Privacy Rule and defines the specific actions that must be implemented at the system level and/or by individual covered entities within the SHCC in order to meet the requirements of The Standard.

Footnotes. The Privacy Rule states that covered entities have “flexibility and workability” in order to implement the Rule and not interfere with access to care. As such, the Privacy Rule does not always provide specific answers to the myriad array of issues that arise within a complex University setting. The University believes that the Privacy Rule provides covered entities with discretion, under the oft-stated HIPAA principles of flexibility and workability, to interpret the regulations so long as one can reasonably support the interpretation. Footnotes provide reference to the regulatory language, the Preambles to the rules or to guidance provided by the Department of Health and Human Services.

Appendix A: Members of the University’s HIPAA Taskforce

Appendix B: University’s HIPAA Implementation Packet: List of Items

Appendix C: Glossary of Terms
III. HIPAA PRIVACY RULE STANDARDS

Standard One: The Organizational Requirements of a Covered Entity

- Designate the University of California Covered Entities and Workforce Members Within the Single Health Care Component (SHCC)
- Establish the System Standards and HIPAA Policies
- Designate Privacy Official(s) and Individuals Designated with the Responsibility for Implementation of the Privacy Rule
- Train the Single Health Care Component Workforce.
- 45 C.F.R. 164.504, 164.514, 164.530

HIPAA covers health plans, health care clearinghouses or those healthcare providers that transmit health information (directly or through an intermediary) electronically for one or more of the following:

1. Benefit coordination;
2. Health care claims or encounter information;
3. Payment and remittance advice;
4. Health care claim status;
5. Health plan eligibility;
6. Enrollment and disenrollment;
7. Health plan premium payments;
8. Referral certification and authorization;
9. First report of injury;
10. Health claims attachments; and
11. Other transactions involving the transmission of a person’s protected health information.

The Board of Regents of the University of California (UC) has defined itself as a hybrid covered entity\(^1\) with a single health care component (SHCC) that includes all covered individuals and

---

\(^1\) Hybrid Covered Entity is a covered entity that is a single legal entity and that performs both covered and non-covered functions.
entities that must comply with the HIPAA Privacy Rule. Since HIPAA permits a single health care component to use and disclose PHI within the single entity for purposes of treatment, payment and operation, designating the HIPAA-covered entities and individuals within UC as a single health care component provides for enhanced workability of the rule and enables UC to sustain its education mission, reduce the costs of compliance, share best practices and enhance compliance.

Moreover, UC is a hybrid covered entity that performs multiple covered functions\(^2\) as a health care provider and health plan. The covered providers and plans must comply with those requirements applicable to plan or provider functions. However, the fact that UC includes both its covered providers and plans within the SHCC does not allow UC workforce members or entities to use or disclose PHI in any way other than what HIPAA allows if UC providers or plans were separate and distinct covered entities. Workforce members who provide business and finance services to both UC covered healthcare providers and UC health plans cannot use or disclose PHI between those entities unless it is allowed in the Privacy Rule.

**UC MUST DESIGNATE AND DOCUMENT COVERED ENTITIES AND INDIVIDUALS WITHIN THE SINGLE HEALTH CARE COMPONENT (SHCC)**

When the Privacy Rule references “the covered entity,” UC has substituted the term “Single Health Care Component” (SHCC). The Privacy Rule requirements apply only to the University-defined and documented SHCC. The SHCC includes those entities and workforce members that perform covered functions as a:

1. Health care provider or those entities and workforce members who do not necessarily engage in electronic transactions as currently defined, but do otherwise meet the definition of a health care provider;\(^3\)
2. UC’s self-funded group health plans; and
3. Those entities and workforce members who perform business, legal, and administrative and finance activities or functions on behalf of UC’s health care providers or plans when those functions involve the use or disclosure of protected health information that has been created or received by UC’s covered entities (health care providers or health plans).

Identifying those individuals or entities that are a part of the SHCC is complicated by the fact that UC is a hybrid covered entity with multiple covered functions and a mission that includes care, service, education and research. Workforce members often have multiple roles, both covered and non-covered. The determination of those entities and individuals is a dynamic and ongoing process that includes the following criteria:

---

\(^2\) “A covered entity that performs multiple covered functions may use or disclose the PHI of individuals who receive the covered entity’s health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.” December Rule 2000, 45 CFR 164.504 (g).

\(^3\) Fed. Reg. 67:157. August 12, 2002, Page 53206: “A hybrid covered entity may include in its health care component a non-covered health care provider component….if a covered entity decides to exclude from its health care component a non-covered provider, the health care component is then restricted from disclosing PHI to that provider for any of the non-covered provider’s health care operations (e.g., teaching), absent an individual’s authorization.”
1. When the use and disclosure of individually identifiable health information (IIHI)\(^4\) is carried out by UC’s SHCC covered entities and workforce members, the individual’s health information is defined as PHI, and the Privacy Rule covers those functions and workforce members who carry out those functions;

2. When the use and disclosure of IIHI is carried out by a business, financial, legal or administrative entity of the UC on behalf of or for UC’s SHCC, the individual’s information is PHI, and the Privacy Rule covers the functions and workforce members who carry out those functions;

3. When the use and disclosure of IIHI is carried out by UC in its capacity as an employer\(^5\) or an educational institution, the information is not PHI and those UC functions are not subject to the Privacy Rule, but the confidentiality of the individual’s health information is protected by other state and federal law, as well as UC policy; or

4. When the use of IIHI is by a UC researcher for an IRB-approved protocol, the information is not PHI; however, when the researcher wants to use PHI created, received or maintained by the SHCC for purposes of the approved research, the Privacy Rule mandates that the SHCC receive specific assurances that the individual’s health information will be protected once disclosed to the researcher. UC’s Institutional Review Boards (IRB) have determined that they will serve as the required Privacy Board (see Standard Nine).

**UC MUST DESIGNATE A PRIVACY OFFICIAL(S) AND INDIVIDUALS DESIGNATED WITH THE RESPONSIBILITY FOR IMPLEMENTATION OF THE PRIVACY RULE**

The Privacy Rule requires the University to establish policies and procedures that provide for administrative responsibility and to designate at least one privacy official who has overall responsibility and accountability for: the University’s development and implementation of the policies and procedures; receiving complaints under this section; and providing further information about the SHCC’s use and disclosure of PHI as described in the required Notice of Privacy Practices (see Standard Four).

The Privacy Rule mandates the following administrative requirements:

1. Train the workforce and document the training;

2. Implement reasonable institutional and individual safeguards to protect PHI;

3. Provide a process for individuals to make complaints to the SHCC;

---

\(^4\) In the course and scope of employment, UC employees may have occasion to access, use, disclose or maintain health information about an individual or “individually identifiable health information.” While an individual’s health information may be covered by state or federal law other than HIPAA, it only becomes PHI when it is use, created, disclosed or maintained by a HIPAA-covered entity carrying out HIPAA-covered functions.

\(^5\) Fed Reg. 67:157, August 12, 2002, Page 53191. “Covered entities must comply with this regulation in their health care capacity, not in their capacity as employers. For example information in hospital personnel files about a nurse’s sick leave is not PHI ...”
4. Establish and apply appropriate sanctions against workforce members who fail to comply with the Privacy Rule or UC policy and document any applied sanctions;

5. Mitigate, to the extent practicable, any known harmful effect of a violation of the Privacy Rule or policies;

6. Refrain from intimidating or retaliatory acts; and

7. Establish policies and procedures.

The University of California is a 10-campus system with, in most cases, administrative responsibility delegated to the Chancellor of each campus. To provide for administrative efficiency and effectiveness in complying with the requirements of the Privacy Rule, the Board of Regents supported the HIPAA Taskforce’s recommendation that UC implement a single system approach to compliance. In January 2003, the Office of the President designated an individual to serve as the University’s HIPAA Privacy Official. In order to provide for local campus flexibility and management of the requirements of the Privacy Rule, the HIPAA Taskforce recommended that certain required functions be delegated locally, with system reporting to the Board of Regents through the HIPAA Taskforce and University’s HIPAA Privacy Official.

The System Standards Implementation Policy 1-4 describes the responsibilities of the University’s HIPAA Privacy Official and the campus Privacy Officers or Liaisons. To provide for local compliance with these administrative requirements, the HIPAA Taskforce has recommended to the Board of Regents that each Chancellor should also designate one or more Privacy Liaisons. This requirement can be met by one of the following:

1. At those campuses that have academic health centers designate both a Privacy Officer or Official responsible for the compliance activities of the academic health centers and another individual or individuals who would be accountable to the Chancellor and serve as liaison to the HIPAA Taskforce and University HIPAA Privacy Official for those activities described in Implementation Policy 1-4. In some cases, the campus Privacy Liaison may be more than one person. For example, the Chancellor might appoint both the Director of Student Health Services and an individual from the Chancellor’s immediate office to cover the responsibilities;

2. At those campuses that do not have an academic health center, designate one or more individuals who are accountable to the Chancellor and serve as liaison to the HIPAA Taskforce and University HIPAA Privacy Official for those activities described in Implementation Policy 1-4. In some cases, the campus Privacy Liaison may be more than one person; for example, the Chancellor might appoint both the Director of Student Health Services and an individual from the Chancellor’s immediate office to cover the responsibilities; or

---

6 Board of Regents’ Resolution, May 2002

7 Maria Faer, DrPH, University Privacy Official and Chair of the University’s HIPAA Taskforce.

8 UC Davis, UC Irvine, UC Los Angeles, UC San Diego, UC San Francisco
3. Request that the University’s HIPAA Privacy Official also serve as the Campus Privacy Liaison, providing the Chancellor with information necessary to assure local compliance.

**UC MUST ESTABLISH POLICIES AND PROCEDURES WITH RESPECT TO THE USE AND DISCLOSURE OF PHI**

The SHCC must implement policies and procedures with respect to the use and disclosure of PHI. As allowed by the Privacy Rule, the SHCC, in developing these Systemwide HIPAA Policies, has taken into account the requirements of the Privacy Rule that policies and procedures be “reasonably designed, taking into account the size of and the type of activities that relate to PHI undertaken by the covered entity.”

Moreover, because UC is a hybrid covered entity with multiple covered functions (health care provider and health plan) and a tripartite mission of care/service, education and research, the challenge to implement the requirements of HIPAA are greater than for those entities that are single covered entities. For example, in many cases, UC workforce members will perform business and/or finance services for both the UC’s covered health care providers or plans (i.e., the SHCC) and for UC entities that are not covered under HIPAA (i.e., not a part of the SHCC). When workforce members or UC divisions provide services for both the SHCC and non-covered UC entities, only those business and finance functions provided for the SHCC, rather than entire units or departments, are subject to HIPAA. In these cases, UC has endeavored to identify these individuals, provide education and develop policies and procedures that will help establish a “firewall” to prevent the use and disclosure of PHI between the SHCC and non-SHCC. The disclosure of PHI between the SHCC and non-SHCC of the hybrid covered entity will require, in almost all cases, the individual’s written authorization.

**UC MUST TRAIN ALL HIPAA-COVERED WORKFORCE MEMBERS**

The Privacy Rule requires training of all members of the SHCC workforce of the SHCC regarding policies and procedures with respect to HIPAA and PHI. This includes initial training prior to the time that the rules become applicable, with subsequent training of new staff and retraining as changes occur within either HIPAA or UC policies and procedures. All members of the workforce of the SHCC must be trained, including faculty, employees, volunteers, trainees, and any others “directly controlled” by the SHCC. Documentation of the training must be kept in written or electronic form for six years. For purposes of determining the scope of the training required, UC has defined all those who work or volunteer within the SHCC covered entities, even if they are temporary or infrequently a part of the workforce as members of the workforce, and will provide training in the SHCC’s HIPAA policies and procedures.

---


10 For example, visiting or volunteer faculty who on occasion participate in teaching or care are considered workforce. Students from allied professional schools (e.g., physical therapy, technologists, nursing, social welfare) who rotate through the SHCC as a part of their required training will be considered part of the SHCC workforce when within the covered entity.
STANDARD ONE: IMPLEMENTATION POLICIES

Implementation Policy 1-1: Designation of Covered Entities in the SHCC

The Board of Regents has designated the following UC entities and workforce members as part of the UC Single Health Care Component (SHCC) and, as such, subject to the HIPAA Privacy Rule and UC’s System Standards:

1. The five Academic Health Centers, medical centers and clinics at Davis, Irvine, Los Angeles, San Diego, San Francisco;

2. Health professional schools at Berkeley, Davis, Irvine, Los Angeles, San Diego, San Francisco:

3. Functions within the three UC-administered Department of Energy Laboratories at Berkeley, Livermore, Los Alamos, including occupational health;

4. Student Health Centers at all campuses;

5. Athletic Departments at some campuses;

6. Occupational Health Centers at some campuses;

7. UC self-insured health or group health plans;

8. Certain department sponsored clinics providing health care to the community as a part of the education and research missions of those departments (e.g., behavioral health, speech and hearing services, etc.);

9. System and campus Privacy and Compliance Offices, HIPAA Taskforce and Covered Entities’ HIPAA committees (Systemwide and campus) and Corporate Compliance Committees (Systemwide and campus); and

10. Other UC entities engaged in covered functions and which use and disclose PHI as determined by the Board of Regents.

Implementation Policy 1-2: Designation of UC Workforce Members Who May Provide Business, Finance, Legal or other Services to Covered Entities.

The following entities and their workforce members in the UC Office of the President (UCOP), at UC campuses and Department of Energy (DOE) laboratories administered by UC may provide business, legal, financial or administrative functions on behalf of the SHCC and are part of the SHCC when performing those functions that require the use and/or disclosure of PHI on behalf of the SHCC:

1. Office of the General Counsel;

2. Office of Business and Finance and University Auditor;

3. Office of Clinical Services Development;
4. Office of Health Affairs;
5. Office of External Relations;
6. Institutional Advancement or Development Office;
7. Board of Regents;
8. Institutional Review Boards and individual UC Researchers;
9. Information Technology and Office of Technology Transfer; and
10. Other UC entities that perform covered functions for entities within the SHCC as determined by the Board of Regents.

When these workforce members perform services on behalf of non-covered entities within UC, these functions are not part of the SHCC. Workforce members must not disclose PHI to non-covered UC entities without the individual or patient’s authorization, as required by the Privacy Rule.

**Implementation Policy 1-3: UC Entities and Individuals Who May Use or Disclose an Individual’s Identifiable Health Information (IIHI), But Are Not Part of the SHCC.**

The Privacy Rule does not apply to the employer or certain academic administrative functions of UC and to employment and student records as defined. When UC is caring out its role as an employer, those workforce members providing these services or functions are not subject to the requirements of HIPAA, except when UC, the plan sponsor, has certified to the insured health plans that PHI will be protected as defined in the plan documents (see Section IV.) To obtain PHI from covered entities within the SHCC, UC, in its role as employer must, with certain exceptions, obtain written authorization from the individual. This restriction is particularly sensitive when the patient is a UC employee within the SHCC. Further, such information may be subject to other federal or state laws that provide for confidentiality. Examples of UC entities and workforce members that are not part of the SHCC and are not covered by HIPAA are the Employee Assistance Programs, academic admissions offices, and Disability and Worker’s Compensation Managers.

---

11 For example, UC employees who work in the campus admissions office or student assistance offices may use individually identifiable health information in their capacity as admissions officers or individuals who provide services to students requesting special academic, housing or meal accommodations for medical reasons. UC has determined that those are non-covered functions under HIPAA, although state and federal law regarding the protection of student records will apply.

12 See Standard Two: PHI for a description of employment records not included in the definition of PHI.

13 The SHCC may disclose PHI to the employer under limited circumstances—e.g., medical surveillance of the workplace or to evaluate work-related injury or illness, or its obligations under 29 CFR parts 1904-1928, 30 CFR parts 50-90, or other state law so long as the covered health care provider gives notice in the Notice of Privacy Practices that this disclosure will occur and provides an accounting of this disclosure to the individual if the individual requests an accounting. Privacy Regulation Text, October 2002, p. 16.
However, in all these cases, either state or federal law and/or UC policy provides for confidentiality of that information and prohibits the use of an individual’s health information for employment-related decisions. The fact that the Privacy Rule does not apply does not lessen any current protections for that information, and, in the case of those individuals such as benefits managers, customer service representatives or health facilitators, the UC plan sponsor must certify to the health plan that information will not be used for employment-related decisions and that those individuals will provide the Privacy Rule required protections for an individual or member’s health information.

**Implementation Policy 1-4: Privacy Official(s), Campus Privacy Liaisons and Privacy Office.**

The University of California must designate a SHCC Privacy Official who also serves as the University’s contact person and contact office. The Chancellor of each campus is also responsible for designating the individual(s) who will be accountable to the Chancellor for campus compliance with HIPAA and serve as the campus liaison(s) to the system HIPAA Taskforce.

The responsibilities of the University’s HIPAA Privacy Official include:

1. Document the personnel designations for all covered institutions within the SHCC as required by the Privacy Rule and maintain copies of the job descriptions, contact numbers and addresses for all University HIPAA Privacy and Security Officials or Officers and Liaisons;

2. Oversee all ongoing activities related to the development, implementation, maintenance of and adherence to UC’s policies and procedures covering the privacy of and access to patient health information in compliance with the Privacy Rule;

3. Serve as the SHCC’s contact person responsible for receiving complaints and providing information regarding the SHCC’s HIPAA privacy practices as described in the SHCC’s Notice of Privacy Practices;

4. Maintain current knowledge of applicable federal and state privacy laws and coordinate with other UC divisions regarding federal and state laws and the institution’s privacy practices that may impact the University’s compliance with the Privacy Rule;

5. Modify and update all Privacy Rule policies and the Notice, in consultation with the Office of the General Counsel and System HIPAA Taskforce, if required by changes in federal or State law or as needed to respond to UC policy changes;

6. In consultation with the System HIPAA Taskforce, develop mechanisms that provide assurance to the Board of Regents that the Privacy Rule required documentation is accomplished and maintained by the appropriate covered entities within the SHCC and at the system level;

7. Coordinate with system or local Compliance Officers, the Office of the General Counsel, Office of Risk Management, the University Auditor, campus Privacy Officers and Liaisons and others as necessary to provide a response to individual complaints, identify and mitigate potential violations and apply and document appropriate sanctions for failures by the workforce to comply with the Privacy Rule and the System HIPAA Guidelines and local policies and procedures (*See Standard Sixteen*);
8. In coordination with the HIPAA Taskforce, develop a process for using complaints as evaluative and improvement tools;

9. Develop, in coordination and consultation with the System HIPAA Taskforce, workforce training and develop a process to provide assurance to the Board of Regents that required training and documentation have been met;

10. Maintain records of HIPAA education materials developed and implemented by the University’s HIPAA Taskforce;

11. Maintain records of the University HIPAA Privacy Official’s job description, location of the system Privacy office or contact person and comparable documentation for each of the ten campuses’ and the five academic health center Privacy Officers, Liaisons, Office and contact person (s);

12. Cooperate with complaint investigations and compliance reviews;

13. Permit access to information as required by DHHS and permitted under the Privacy Rule;

14. Where applicable, organize, manage and manage a HIPAA Privacy Office and the HIPAA Taskforce; and

15. Report, as appropriate, at the local and system level to executive management and to the Board of Regents as required by local or system policy.

The HIPAA Taskforce recommends that each Chancellor designate one or more individuals responsible for carrying out the following responsibilities in coordination with the efforts of the Systemwide HIPAA Taskforce and UC’s HIPAA Privacy Official:

1. Manage the development and implementation of campus or academic health center policies and procedures necessary for carrying out the requirements of the System Standards, HIPAA System Policies and the Privacy Rule and the education of the campus workforce with respect to the Privacy Rule;

2. Document all training in written or electronic form and retain the records for at least six years. Documentation, at a minimum, must be either: a) by individual; b) by workforce category; or c) department or division;

3. Certify on an annual basis to the HIPAA Taskforce and UC HIPAA Privacy Official that required workforce training and documentation standards have been met; and

4. Serve as the campus or academic health center liaison (s) to UC’s HIPAA Taskforce;

5. Serve as the campus or academic health center individual (s) responsible for assuring that HIPAA required mitigation, complaint, and sanction standards and policies are implemented and documented;

6. In coordination with the HIPAA Taskforce, determine who will access complaint information and for what purposes in order to use complaints as evaluative and improvement tools;
7. Serve as the campus or academic health center contact person(s) responsible for receiving complaints and providing information regarding the campus’s HIPAA privacy practices;

8. Modify and update all Privacy Rule policies and the Notice as determined by the System HIPAA Taskforce and required by changes in federal or State law or as needed to respond to UC policy changes;

9. Assure that the Privacy Rule required documentation is accomplished and records maintained by the campus or academic health center and provide certification to the Board of Regents or management as required in local or system policy;

10. Develop a campus or academic health center policies and process to provide for required workforce training and documentation of the training;

11. Maintain records of the campus or academic health center’s Privacy Officer or Liaison’s job description and, where appropriate, location of the Privacy office or contact person.

12. Cooperate with complaint investigations and compliance reviews;

13. Permit access to information as required by DHHS and permitted under the Privacy Rule; and

14. Report at the local and system level to executive management and others as required by local or system policy.

Implementation Policy 1-5

Each entity within the SHCC will train its workforce members on the System Standards and local policy and procedures prior to the effective date of April 2003. Each entity within the SHCC shall provide a program to train new employees, faculty, trainees, students, volunteers and other workforce members reasonably soon after they join the University, but no later than 90 days. When significant changes occur in the job description of current employees or policy and/or procedures, the affected workforce members will be trained as soon as possible after such changes. The local Privacy Officer(s) or Liaison(s) is responsible for implementing the required training.

Implementation Policy 1-6

Members of the workforce who function at multiple locations or in multiple covered entities need be trained only once initially, provided the Privacy Official or Liaison at the entity within the

---

14 The SHCC has defined “workforce members” as those faculty, trainees, students, volunteers and others paid or unpaid, whose performance is under the control of the SHCC. Within the academic health center environment, visiting faculty or community physicians with medical staff privileges often participate in the treatment and/or health care operations of the SHCC. In most cases, the SHCC has determined that those individuals are part of the SHCC workforce and are not business associates of the SHCC because they are performing current treatment and/or teaching activities under the direct control of the SHCC. These individuals will receive HIPAA training as determined by the campus or UC HIPAA Privacy Official. When these individuals are performing covered functions for covered entities that are not part of the UC’s SHCC, they are not part of the SHCC workforce and are individually responsible for complying with the requirements of HIPAA.
SHCC has approved the training program and has documented that the individual has received training. This is particularly applicable to those health professional program undergraduate and graduate students (Schools of Medicine, Nursing, Optometry, Public Health, Dentistry and Pharmacy) who receive health professional training and participate as part of the health care provider team at multiple training sites. When the training sites are at other covered entities affiliated with the SHCC for teaching purposes, one education session provided by any one of the covered teaching institutions will suffice so long as the academic health center or system Privacy Official has certified that the training provided meets the standards established by the SHCC. The SHCC should amend affiliation agreements with covered teaching entities and service agreements to reflect these requirements and provide documentation that the Privacy Rule education requirements have been met.

**Standard Two: Protected Health Information (PHI) and Data Sets**

- Protected Health Information (PHI)
  - Student Records
  - Employment Records
- Research Health Information (RHI)
- Designated Record Set (DRS)
- Limited Data Set (LDS) and Data Use Agreement
- Deidentified Data
- CFR 160.103, 164.501, 164.502, 164.514, 164.528

**Definition of Protected Health Information (PHI)**

Protected Health Information is an individual’s health information that:

1. Created or received by a health care provider, plan, or clearinghouse;

2. Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual;

3. Identifies the individual, or is reasonably believed could identify the individual; and

4. Is transmitted or maintained in any form or medium.

PHI excludes Education Records covered by FERPA and Employment Records Held by UC in its Role as Employer. HIPAA excludes Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g and, specifically, records described at 20 1232g(a)(4)(B)(iv) as follows:
“Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student’s choice.”

For purposes of designating those entities and records covered by HIPAA, UC has determined that:

1. An individual’s health information contained in the health records of a student attending a UC institution of postsecondary education is excluded from FERPA when defined under FERPA’s exception, and FERPA requirements with respect to the release of a student’s education records do not apply to those health records as defined in 20 1232g(a)(4)(B)(iv) and for the purposes as defined under that section;

2. The UC Student Health Services provide health care to both students and non-students on a frequent basis. Operationalizing a system that would subject students to a different standard than that for non-students would be costly, potentially place UC a risk if employees could not readily make the distinction between students or non-students, and potentially cause patients—both students and non-students—to raise questions or concerns if they did not understand the reason for what might appear to be a double standard—e.g., why does one individual receive Notice and request for a Written Acknowledgment and another individual does not?

3. Since the Privacy Rule allows UC, a hybrid covered entity, to include non-covered health care providers in the SHCC, the Student Health Services have recommended to the HIPAA Taskforce and Regents that it provides for more flexibility, workability and will enhance compliance if the Student Health Services and those health records maintained by Student Health Services as described at 20 1232g(a)(4)(B)(iv) are subject to HIPAA; and

4. All other education records, as defined under FERPA, which may contain a student’s individually identifiable health information as required in the admissions or other similar academic process, are not subject to HIPAA, but must meet all requirements of FERPA and other state and federal laws for the release of information.

**UC Policies Applying to Campus Activities, Organizations and Students**

A UC student is defined, according to UC Policy as “an individual for whom the University maintains student records and who is: 1) enrolled in or registered with an academic program of the University; 2) has completed the immediately preceding term, is not presently enrolled and is eligible for reenrollment; or 3) is on an approved educational leave or other approved leave status, or is on filing-fee status.”

---

15 Section 130.
EMPLOYMENT RECORDS HELD BY THE SHCC IN ITS ROLE AS EMPLOYER.

Although an individual’s identifiable health information contained in employment records is not subject to the Privacy Rule, the Rule does not provide a specific definition for “employment records.” Therefore, for purposes of complying with HIPAA, the University has defined employment records as follows and the health information maintained in those records as individually identifiable information (IIHI):

“The University’s employment records include those records held by the University in its role as employer or information used by the employer to take appropriate action as permitted or required by other state or federal law relative to an employee’s health or well being in the workplace and include, but are not limited to, medical information needed for an employer to carry out its obligations under16:

1. Family Medical Leave Act;
2. American With Disabilities Act;
3. OSHA;
4. Workers compensation17;
5. Files or records related to occupational injury;
6. Disability insurance eligibility;
7. Sick leave requests and justifications;
8. Drug screening results;
9. Workplace medical surveillance;
10. A doctor’s statement to the employer to document sick leave;
11. Fitness-for-duty test results of employees; or
12. Other work or employment records containing IIHI, including student/employee records of UC students when employment is contingent upon whether she or he is a student (e.g., workstudy program records are student records) whether released to UC under an authorization or other means allowed by law.”

ANALYZING WHEN AN INDIVIDUAL’S HEALTH INFORMATION IS PHI

The key determinants as to whether or not information is IIHI and not protected by the Privacy Rule or PHI and protected are: 1) the function being performed by UC (employer, provider, health

16 August 2002 version of the Final Rule, p. 23 of 216 pages.
17 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90
plan); and 2) the purpose for which the entity or UC workforce member has received, created or maintained the medical information (treatment, payment, operations, other). Record keeping practices are not the determinant\(^\text{18}\). For example, the results of a fitness for duty exam are PHI when UC as a provider and part of the SHCC administers the test to a UC employee. When the employee authorizes UC, the health care provider, to turn over the information to UC, the employer, it is a part of the employee’s employment record and no longer PHI. It is important to note that in most circumstances (see UC’s Notice of Privacy Practices for exceptions, including workplace injury, illness or medical surveillance), the employee must provide a signed Authorization to the UC health care provider to release the information to UC, the employer.

**REQUIRED DISCLOSURES BY THE SHCC TO THE UC, THE INDIVIDUAL’S EMPLOYER**

The SHCC may disclose PHI to the UC employer, without an individual’s authorization or an opportunity to object, when the use and disclosure is for public health activities, in order to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury, so long as the PHI that is disclosed to the employer consists of findings concerning the work-related illness, or injury or to comply with federal law\(^\text{19}\) or similar state law. The SHCC’s Notice of Privacy Practices must provide written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries may be disclosed to the employer. The Notice must be provided at the time of health care delivery or by posting the Notice at the site of delivery (e.g., occupational health clinic).

Likewise, workforce members or entities that carry out industrial hygiene, health physicist and safety engineering functions will create and use IIHI. These functions are on behalf of UC, the employer, and meet other federal and state laws or requirements.\(^\text{20}\) The IIHI resides in employment records. Therefore, the use and disclosure of IIHI in these circumstances are not subject to the Privacy Rule, but may be subject to other federal and state privacy or confidentiality laws or regulations.

**RESEARCH HEALTH INFORMATION (RHI)**

Research Health Information is a term used by UC to assist the SHCC and researchers distinguish between IIHI that is used for research purposes and IIHI that, due to the nature of the research, is both RHI (IIHI used in the research setting) and PHI (because it is IIHI created in the course of a research protocol that also involves treatment) and should be recorded in the individual’s Designated Record Set. See Standard Nine for an additional discussion recording research.

**DESIGNATED RECORD SET (DRS)**

The Designated Record Set is a group of records that includes PHI. The UC SHCC or covered entity maintains, receives, uses or disseminates the information contained in a DRS for each individual that receives care or is a member of a health plan. Individuals who are patients or


\(^{19}\) 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90.

\(^{20}\) CFR 835.
members have certain rights relative to their DRS (See Standards Eleven through Sixteen). The DRS includes:

1. The medical records and billing records about individuals maintained by or for a covered health care provider (can be in a business associates records);

2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; and

3. That is used, in whole or in part, by or for the covered entity (SHCC) to make decisions about individuals.

Any research activities that create PHI should be maintained as a part of the DRS and are accessible to research participants unless there is a Privacy Rule permitted exception. (See Standards Nine and Thirteen).

The DRS can have subparts contained in more than one location, at more than one covered entity within the SHCC (e.g., UCSD and UCI could both have provided care to an individual and maintain separate medical records) and in more than one format, including computer databases, hardcopies, and databases created and maintained by the business associate. However, exercising ones privacy rights relative to the DRS, the individual must take responsibility for identifying and contacting the different covered entities within the SHCC that may have provided care or served as the members’ plan.

EXCLUSIONS FROM THE DRS

The DRS does not include:

1. Back-up information used in the billing process;

2. Information used solely in health care operations;

3. Working or teaching notes (including a student’s notes, note cards and PDA’s notes) or other similar documents. In these cases it is the responsibility of the individual to ensure that the medical record or DRS is not removed from the SHCC, to transfer any denova PHI to the DRS and to provide for physical safeguards for any information contained in those working or teaching notes or for the devices themselves;

4. Peer review information protected by California Evidence Code 1157 or other confidential or privileged information;

5. Appointment or surgical schedules or other operational information; or

6. Oral communications dealing with treatment, payment or operations, unless, by its nature, it is necessary to make decisions about the individual and should be included in the DRS (e.g., a phone call to report a communicable disease should be included in the DRS and, thereby, be available for an individual’s inspection or account disclosure when requested by the individual).
DEIDENTIFICATION OF PHI

Deidentification of PHI creates a Deidentified Data Set which is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. The SHCC does not need the patient’s signed Authorization to use or disclose a Deidentified Data Set and does not have to provide the patient with an accounting of uses and disclosures of deidentified data.

The Deidentified Data Set can be used for any purpose, including research, media communications, teaching of students outside the clinical setting or CME courses, where the SHCC would normally require the individual’s signed Authorization for use or disclosure of the PHI. The National Bioethics Advisory Commission describes this as “coded data” in its guidelines on genetic research for IRBs. The Office of Human Research Protection has adopted that guideline for all research under its auspices.

The SHCC creates a Deidentified Data Set by removing the following 18 identifiers of the individual or of relatives, employers, or household members of the individual:

1. Name;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account Numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);

15. Internet Protocol (IP) address numbers;

16. Biometric identifiers, including finger and voiceprints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code.

De-identification can also be accomplished if a person with appropriate knowledge and experience applies generally accepted statistical methods to render information as not individually identifiable and documents that there is only a small risk of the recipient of the PHI being able to re-identify the individual. The SHCC can assign a code or other means of record identification to allow information deidentified to be reidentified by the SHCC so long as the code is not derived from or related to information about the individual and capable of being translated so as to identify the individual and the SHCC provides for security of the code. The code cannot be derived from any of the elements removed to effect de-identification.

When a researcher wants to use a Deidentified Data Set for the research purposes, the Institutional Review Board (IRB) will approve de-identification proposals. (See Standard Nine).

**LIMITED DATA SET (LDS) AND THE DATA USE AGREEMENT**

The SHCC may use or disclose a Limited Data Set (LDS) for research (e.g., research data base), public health or health care operations (e.g., CME courses, undergraduate medical education courses with no clinical rotation) without the individual’s signed Authorization and or provide an accounting of the disclosures so long as the SHCC enters into a Data Use Agreement with the recipient of the LDS. When the recipient of the LDS is a UC employee, including faculty member or researcher, s/he may create the LDS acting as a member of the SHCC workforce so long as s/he has received UC’s required Privacy Rule training. The UC employee may also be the recipient of the LDS s/he has created so long as s/he enters into the UC Confidentiality Agreement that contains elements of a Data Use Agreement. By doing so, the employee affirms that s/he will protect the LDS s/he has received from the SHCC.

Uses of the LDS may include:
1. Public health uses include disease registries maintained by private organizations and not covered by government regulations;\textsuperscript{21}

2. Human subjects research with an IRB approved protocol that allows for a Limited Data Set; and

3. Teaching activities, including undergraduate medical education and non-clinical settings and those students from non-UC allied professional schools who may next health information as part of their training purposes.

The IRB will approve the use of a LDS for research. Each covered entity within the SHCC is responsible for identifying the individual(s) responsible for entering into Data Use Agreements and maintaining copies of the agreements. The following 12 direct identifiers must be removed from the PHI to create the LDS:

1. Name;
2. Street address or postal address, other than city, state and zip code (different than Deidentified Data Set);
3. Telephone and fax numbers;
4. E-mail address;
5. Social Security Numbers;
6. Certificate/license numbers;
7. Vehicle identifiers and serial numbers, including license plate numbers;
8. URLs and Internet Protocol addresses;
9. Full face photos and any other comparable images;
10. Medical record numbers, health plan beneficiary numbers and other account numbers;
11. Device identifiers and serial numbers; and
12. Biometric identifiers (voice and finger prints).

Under a Limited Data Set, researchers and others have access to full dates of admissions and discharge, birth and death, as well as five-digit zip code or other geographic subdivisions other than street address.

\textsuperscript{21}Fed. Reg. 67:157, August 12, 2002, 53236. “...The limited data set provision may permit disclosures for public health activities not allowed under 164.512(b). These might include disease registries maintained by private organizations or universities or other types of studies undertaken by the private sector or non-profit organization for public health purposes.”
DATE USE AGREEMENT

The Data Use Agreement is entered into between the SHCC and the recipient of the LDS when that recipient is not a member of the UC workforce (must sign Confidentiality Agreement with Data Use Agreement elements) and must:

1. Establish the permitted uses and disclosures of the LDS;
2. Establish who is permitted to use or disclose the LDS;
3. Limit redisclosure by the recipient except as permitted in the Agreement or required by law;
4. Require the recipient to agree not to re-identify the data or contact the individual;
5. Contain adequate assurances that the recipient will use appropriate safeguards to prevent use or further disclosure of the limited data set, except as permitted;
6. Report to the SHCC any use or disclosure not provided for in the agreement;
7. Ensure that any agents to whom the recipient provides the LDS agree to the same restrictions and conditions that apply to the recipient

The University’s HIPAA Implementation Packet includes a Data Use Agreement. Individuals who want to create or use a LDS should consult with medical records or the local Health Information Management Systems or Privacy Management Office, IRB, Office of the General Counsel, local Privacy Official or University HIPAA Privacy Official.

STANDARD TWO: IMPLEMENTATION POLICIES

Implementation Policy 2-1

When an individual requests access to or copies of medical records or PHI in the Designated Record Set (DRS), the covered entity or individual that receives the request is only responsible for providing the copy of the DRS that is maintained or stored within that entity (e.g., one medical center or physician office). The patient or individual requesting access is responsible for identifying his/her health care providers and providing separate requests to each of the covered entities for access to or copies of his/her records. However, each covered entity (e.g., one medical center) is responsible for providing the individual with access to the full DRS that is maintained by the covered entity, even if it is located within different departments in the covered entity.

Implementation Policy 2-2

SHCC workforce members cannot remove the DRS from the care delivery site. Copies of an individual’s health information contained in teaching or treatment notes and stored on laptops and PDAs may be removed from the UC worksite so long as the workforce member is personally responsible for providing appropriate and reasonable safeguards to protect the information contained on those portable devices.
Implementation Policy 2-3

Covered entities within the SHCC will adopt local policies and procedures to provide for the deidentification of data, creation of a LDS, and providing for an appropriate Confidentiality Agreement of Data Use Agreement where required. The SHCC is not required to track disclosures using a deidentified or LDS set nor obtain the individual’s signed authorization.

Implementation Policy 2-4

For research purposes, the use of a LDS and the elements of the Data Use Agreement will be reviewed and approved by the IRB as part of their protocol approval process.

Implementation Policy 2-5

In order to create a LDS, the SHCC may:

1. Allow members of the University’s workforce —e.g., a UC researcher, faculty member or other LDS recipient—to create the LDS, acting as a member of the SHCC’s workforce who has received required Privacy Rule training; or

2. Train members of the SHCC workforce to create the LDS (e.g., medical records); or

3. Hire a business associate to create the LDS through a business associate agreement.

Implementation Policy 2-6

In order to receive a LDS for research, public health or operational purposes (including CME course or other teaching purposes), UC workforce members must either enter into a Confidentiality Agreement that contains the required Data Use elements or a Data Use Agreement as required under the Privacy Rule.

Implementation Policy 2-7

The SHCC is not responsible for violations of the Data Use Agreement, but if the SHCC knows of a pattern of activity or practice that constitutes a material breach or violation of the agreement, then it must take reasonable steps to cure the breach or end the violation or withhold the LDS. If this is not possible, the breach should be reported to the Secretary. If the recipient of a LDS under a Data Use Agreement is a covered entity (e.g., a member of the SHCC’s workforce or an outside covered entity), a breach of the Data Use Agreement is a violation of the Privacy Rule.

Implementation Policy 2-8

The SHCC may reasonably rely on a requested disclosure using a LDS as the minimum necessary.

Implementation Policy 2-9

In order to create a Deidentified Data Set, the SHCC may allow the recipient of the data set to do so, train designated workforce members (e.g., medical records or HIMs), engage a business associate, or establish an expert panel or resource within the SHCC to assist in the de-identification of PHI.
Standard Three: Safeguards for Protected Health Information (PHI) Institutional Safeguards

- Individual Safeguards
- 45 C.F.R. 164.504, 164.530

Institutional Safeguards

The University must provide reasonable and appropriate administrative, technical and physical safeguards for PHI in accordance with the requirements of the Privacy Rule, including the System Standards, campus-specific policies and procedures, and HIPAA workforce education programs. On December 3, 2002, the Office of Civil Rights published additional guidance to suggest practices that entities and individuals can use to provide for reasonable safeguards, 22 and the SHCC has taken those recommendations into account when developing the policies and procedures.

Individual Safeguards

Each member of the SHCC workforce is individually responsible for meeting the SHCC’s requirements for obtaining training necessary to carry out individual job responsibilities that involve the use and disclosure of PHI, for seeking assistance if questions or concerns arise regarding the use and disclosure of PHI and for immediately reporting known or suspected violations (accidental, erroneous or deliberate) to the UC HIPAA Privacy Official or local Privacy Officers or Liaisons so that, to the extent possible, UC can mitigate any known harmful effects of the violation.

Standard Three: Implementation Policies

Implementation Policy 3-1

Members of the SHCC workforce will only use and disclose PHI as permitted under the Privacy Rule and must not disclose PHI to workforce members who are not part of the SHCC, except as specifically allowed under the Privacy Rule and state law and, in most cases, with the individual, member or patient’s signed authorization.

Implementation Policy 3-2

Members of the UC workforce who perform duties for both the SHCC and for those units within UC that are not part of the SHCC can only use and disclose PHI in the course and scope of their job duties as allowed by the Privacy Rule. The workforce member cannot use PHI for activities or functions outside of the SHCC unless it is otherwise permitted or required by law or the individual, patient or member has provided a written authorization for the disclosure of PHI to non-covered entities within the University.

**Implementation Policy 3-3**

When a Privacy Rule violation—an improper use or disclosure of PHI is the result of an innocent mistake, neglect or is deliberate—the SHCC must have in place a mitigation process to minimize the effect on the individual of the violation, to comply with state law regarding the notification of individuals, and to prevent future reoccurrences. This process will include, where workable and practicable, efforts to:

1. Contain the damage and stop further use or disclosure;
2. Retrain employees to prevent future mistakes or errors;
3. Apply discipline or sanctions as required under UC policy;
4. Utilize violations as a means to identify system lapses and to modify policies or procedures; and
5. Inform patients, where appropriate, of any improper use or disclosure arising from a violation of the Privacy Rule.

**Implementation Policy 3-4**

Each member of the SHCC’s workforce must be aware of those types of oral or written communications that could result in the unintentional disclosure of PHI to those not permitted to receive PHI and for applying reasonable safeguards to prevent unintentional, careless and illegal access to or use of PHI.

**Implementation Policy 3-5**

The SHCC should provide for technical and physical safeguards to protect PHI in oral, written and non-electronic forms.

---

**Standard Four: Required Notice of Privacy Practices and Written Acknowledgment of Receipt**

- Uses and Disclosures Of PHI That Do Not Require Notice.
- A Patient’s Right To Request Restriction On The Uses and Disclosures of PHI.
- A Patient’s Right to Opt out of the Facility Directory.
- Patient Representatives
- 45 C.F.R. 164.506, 164.510, 164.520, 164.522 and 164.530
Notice of Privacy Practices (The Notice)

The Privacy Rule gives individuals a right to be informed of the privacy practices of their health care providers and health plans, as well as to be informed of their privacy rights with respect to their personal health information. The Privacy Rule requires the SHCC to describe in detail the uses and disclosure of PHI that may be made by the SHCC, the individual’s rights relative to those uses and disclosures, and the SHCC’s legal duties with respect to that information. Consequently, all SHCC uses and disclosures of PHI must be consistent with that Notice. The University’s Office of the General Counsel, in consultation with the HIPAA Taskforce, has prepared the SHCC’s Notice(s)—Medical Notice, Mental Health Notice and Health Plan Notice. The model Notice(s) contains all Privacy Rule required elements and, for this reason, must not be altered or modified without the express review and approval by UC’s Office of the General Counsel.

No later than the date of first service delivery, the SHCC must provide all individuals who receive health care from a SHCC provider (institutional or individual) or who are members of a UC self-funded health plan with the Notice. So long as the SHCC has made its best effort to provide a Notice in plain language, it is not the SHCC’s responsibility to ensure that individuals understand the Notice. The individual has a responsibility to initiate a discussion about the use and disclosure of information, and the regulations do not require the patient to read or understand the Notice.

In an emergency situation, the SHCC must provide the Notice as soon as reasonably possible. The SHCC does not need to obtain a signed acknowledgement in an emergency situation. Inmates do not have a right to a Notice.

The Notice cannot be combined with any other legal permissions or consents. Specifically, the Notice cannot be combined with any HIPAA required Authorization forms.

Although the Privacy Rule generally requires a Notice and Written Acknowledgment before the SHCC uses or discloses PHI, the SHCC can use PHI to schedule appointments and procedures prior to a patient’s first visit. At that visit or “initial moment,” the provider can provide Notice and obtain written acknowledgement. A pharmacist may fill a phone-in prescription for a first-time customer and provide Notice and obtain Acknowledgement when the patient arrives to retrieve the medication.

The Notice may be sent electronically or mailed to the patient. The SHCC may use an electronic or mail return acknowledgement. The patient’s failure to return a signed acknowledgement will not be considered a violation of the “best effort” requirement.

Mental Health Notice

The SHCC has determined that a separate Notice should be provided to individual’s receiving mental health treatment so that patients can be clearly informed about the protections provided for their health information. In many cases, California law provides for more stringent protections of

---

23 August 2002, p. 136

24 Fed Reg. 67,157, August 14, 2002, 53240. “The department would not consider the health care provider in violation of the Rule if the individual chooses not to mail back an acknowledgment.”
these individuals, and the Mental Health Notice takes into account the complex layers of laws relative to these protections. Questions regarding the use and disclosure for Mental Health Patients should be referred to the Office of the General Counsel, local or system Privacy Officer(s) or Privacy Liaison.

HEALTH PLAN NOTICE

The SHCC’s self-funded Health Plans have a Notice that describes the privacy practices for the self-funded plans. The Health Plan Notice will be provided to all plan members no later than April 14, 2003. The Privacy Rule allows the plan to mail the Notice to members, and does not require plans to obtain a written acknowledgement of receipt of the Notice.

INITIAL MOMENT AND SIGNED ACKNOWLEDGEMENT

The Privacy Rule requires that the SHCC use its “best effort” to obtain a signed Acknowledgement from each patient acknowledging receipt of the Notice. In most circumstances, delivery of the Notice and obtaining a signed Acknowledgement should occur at admission or the “initial moment” the covered entity delivers services to the patient. This encounter should offer the patient an opportunity to ask for more information or clarification of the SHCC’s privacy practices and to request restrictions on the use or disclosure of PHI. Health plans and clearinghouses are not required to obtain acknowledgement of the receipt of a Notice. In an emergency situation, the SHCC is not required to obtain a written acknowledgement.

In cases where language or other communication problems prevent obtaining written Acknowledgment, the SHCC must provide Notice to the individual and should indicate that barriers to communication prevented obtaining an Acknowledgment.

The SHCC must document its effort to obtain the Acknowledgement, maintain copies of the written Acknowledgement and document if a patient refuses to provide the Acknowledgement.

RIGHT TO REQUEST RESTRICTIONS

An individual has the right to request restrictions on how the SHCC will use and disclose PHI for those purposes described in the Notice. The SHCC must provide the individual with an opportunity to request restriction of uses and disclosures of PHI and to disclosures to family members, relatives, friends and others. The SHCC has no obligation to agree to the requested restrictions, but will honor all reasonable requests that involve celebrity, patient safety or social stigma. If the SHCC does agree, it must honor the agreed-to-restrictions unless and until they are revoked, except if the individual is in need of emergency treatment. In an emergency, the SHCC may use the restricted information for treatment, but no further disclosures may be made.

The decision to accept a restriction may be an administrative one, covered by policy, or may require review. The campus or system Privacy Officer should review all requests for restrictions that are not authorized by policy or of a questionable nature. The SHCC should implement local procedures that provide a systematic way of communicating restrictions to staff. Never include sensitive information in postcard mailings or send PHI to an unsecured fax machine.

If the requested restrictions interfere critically with patient care, treatment or operations, and the patient is unwilling to modify the request, the entity within the SHCC may decide to refuse to care
for the individual. Issues arising from implementation of this policy will be referred to the Privacy Officer for adjudication. For more information regarding an individual’s right to request restrictions, see Standard Eleven.

**FACILITY DIRECTORY**

A facility directory is the information resource maintained by a covered entity to provide visitors, callers and others with information concerning a patient’s location in the medical facility. So long as the SHCC provides the individual with Notice that certain information will be included in the entity’s Facility Directory and provides the individual with the opportunity to restrict the disclosures, the SHCC may include the individual’s name, location and condition in a facility directory and disclose that information to others who ask for the individual by name. The SHCC may also provide the individual’s religious affiliation to clergy, unless the individual requests that the information not be provided to clergy.

In emergency treatment circumstances that do not require the SHCC to provide Notice to the individual, the individual’s information contained in the Facility Directory may be used or disclosed in accordance with the patient’s prior expressed preference or in the patient’s best interest as determined by the SHCC. In such circumstances, the individual must receive the Notice as soon as practicable and if the individual then objects to use of PHI in the Facility Directory, the SHCC must comply with that request.

**PERSONAL REPRESENTATIVES**

Under the Privacy Rule, a person authorized (under State or other applicable law) to act on behalf of the individual in making health care related decisions is the individual’s personal representative. The Privacy Rule defers to state and other laws in determining who may act on the individual’s behalf. The SHCC should continue to verify an individual acting as personal representatives as they have in the past.

**USES AND DISCLOSURES OF PHI THAT DO NOT REQUIRE NOTICE AND ACKNOWLEDGEMENT OR AUTHORIZATION**

A SHCC can disclose, without notice and written acknowledgment or authorization in the following circumstances:

To the individual who is the subject of the PHI; and

To the Department of Health and Human Services (DHHS) to investigate compliance with the regulations.

**STANDARD FOUR: IMPLEMENTATION POLICIES**

**Implementation Policy 4-1**

Covered entities within the SHCC must implement a Notice and Acknowledgement Process as follows, and the Notice needs to be delivered to the patient only once so long as the individual is a patient of any covered entity or individual within the SHCC.
1. Provide individuals with a written copy of the Notice no later than the date of first service delivery by a direct care provider or in an emergency situation when Notice must be provided as soon as reasonably possible;

2. Make a good faith effort to obtain a written Acknowledgment of receipt of the Notice, except in an emergency situation where no written acknowledgment is required;

3. For over-the-phone first treatment encounters, the SHCC may mail the Notice no later than first service delivery date and include a mail-back Acknowledgment Form;

4. Furnish the electronic Notice automatically and contemporaneously when the first service delivery to an individual is over the Internet, through e-mail or otherwise electronically delivered and make a good faith effort to obtain a return receipt or other transmission from the individual in response to receiving the Notice:
   a) The SHCC may e-mail the Notice to an individual if the individual agrees to receive an electronic Notice. Electronic Notice and Acknowledgment are appropriate for home health care visits so long as they are provided no later than the first day of service;
   b) The SHCC may provide a mailed Notice that contains a tear-off sheet or other document requesting that the Acknowledgement be mailed back to the SHCC. A file copy of the form sent to the patient will be adequate documentation of the provider’s good faith effort to obtain the Acknowledgment. Mailed Notice and Acknowledgment are appropriate in those cases where the health care provider makes home visits. Failure of the individual to return the Acknowledgment is not a violation of the Privacy Rule;

5. Prohibit the combining of the Notice with an Authorization Form or any other legal permissions or consents;

6. When the initial contact is to schedule an appointment, the requirement may be satisfied when the individual arrives at the provider’s facility for the appointment;

7. Post the entire and complete Notice in a clear and prominent location at physical service delivery sites and have it available for individuals to take with them;

8. Retain documentation for six years of the written acknowledgment or of the SHHC’s good faith efforts to obtain acknowledgment;

9. If an Acknowledgment cannot be obtained, the SHCC must document his or her efforts to obtain the Acknowledgment and the reason why it was not obtained; and

10. If there are changes made to the Notice, the SHCC does not have to renotice patients, but must modify the Notice accordingly and make the current Notice (i.e., the one that reflects

---

Pharmacists may obtain the Written Acknowledgment of receipt of the Notice when the individual signs or initials the log book when picking up prescriptions.
any changes in the SHCC’s privacy policies) available at the SHCC’s provider’s office or facility so that individuals can request a copy of the Notice.

Implementation Policy 4-2

Each covered entity within the SHCC has the discretion to design and implement a Notice and Acknowledgement Process that best suits local practice, including the use of mail or email Notices. In all cases where the Notice is not provided in a face-to-face contact, the SHCC must document what procedures it has used to demonstrate a good faith effort to obtain the individual’s written Acknowledgment.

Implementation Policy 4-3

In those situations where an individual is referred to a SHCC provider (direct or indirect) by a non-UC health care provider, the SHCC health care provider should provide the individual with the Notice and make an effort to obtain Written Acknowledgement of Receipt of the Notice.

Implementation Policy 4-4

If, at the direction of the system-wide HIPAA Taskforce, the SHCC’s Notice is modified (e.g., to reflect either regulatory changes or SHCC changes in the use and disclosure of information) the SHCC must post the revised Notice at all physical sites, provide revised Notice upon request and post on the system HIPAA Privacy Web-site. There is no Privacy Rule requirement to re-Notice the SHCC’s patients.

Implementation Policy 4-5

The SHCC may provide the individual with a summary Notice summarizing the individual’s rights, but it can not substitute for the full Notice.

Implementation Policy 4-6

An individual may request restrictions on the use and disclosure of PHI as described in the Notice. Requests for restrictions must be in writing. The SHCC will review all requests and provide the patient or member with a written copy of the SHCC’s decision regarding the request. (See Standard Eleven). The SHCC has no obligation to agree to the requested restrictions, but will honor all reasonable requests that involve celebrity, patient safety or social stigma. The SHCC must honor any agreed to requests for restrictions.

Implementation Policy 4-7

The SHCC must honor an individual’s request to opt out of the Facility Directory (inpatient medical facilities only).

Implementation Policy 4-8

Unwarranted access by a SHCC employee to a fellow employee’s PHI is a violation of the Privacy Rule and UC policy. The Privacy Rule allows access for treatment, payment and some health care operations. If an employee is not required by his or her job description to carryout these activities,
then the UC SHCC policy prohibits access, unless the patient/employee provides written Authorization.

**Implementation Policy 4-9**

The SHCC does not have to witness the individual’s signing of the Acknowledgment or verify the patient’s signature.

**Implementation Policy 4-10**

So long as the SHCC provides the individual with the Notice of the use of the individual’s information in the Facility Directory and provides an opportunity for the individual to restrict the use, the SHCC may include the individual’s name, location and condition in the Facility. If family members, members of the public, or the media ask for an individual by name, the SHCC may disclose the individual’s location and condition so long as the individual has not restricted those disclosures.26

The SHCC may also provide the individual’s religious affiliation to clergy unless the individual objects.

**Implementation Policy 4-11**

Covered entities and individuals within the SHCC should establish policies and procedures for identifying and verifying members of the clergy and routing some inquiries to designated personnel who can handle sensitive cases.

**Implementation Policy 4-12**

In an emergency, the SHCC can use or disclose the individual’s name, location and condition (and religious affiliation to clergy) so long as the SHCC determines that disclosure is in the individual’s best interest, the individual has not previously restricted access nor would do so if given the opportunity, and, as soon as possible, the SHCC will provide the Notice to the individual.

**Implementation Policy 4-13**

In cases where the individual has a personal representative, the provider satisfies the Notice distribution requirements by providing the Notice to the personal representative and making a good faith effort to obtain the personal representative's Acknowledgment of receiving the Notice. In the limited cases where the parent is not the personal representative of the unemancipated minor, such as when the minor is authorized under State law to consent to the treatment and does so, the provider must give its Notice to the minor and make a good faith effort to obtain the minor's acknowledgment of the Notice.

26 For example, if the media learned that a named individual had been injured in an accident, the SHCC could respond to a media query regarding that individual’s condition and location, so long as the media asked for the individual by name.
Implementation Policy 4-14

The SHCC is required by law to provide PHI without the individual’s Authorization or opportunity to object for the purposes of workplace medical surveillance or to report a work-related illness or injury if the SHCC provides written Notice to the individual of this practice. When UC occupational health clinics or other clinics provide these functions on the worksite, the Notice must be provided when the employee receives care or by posting the Notice in a prominent place where the care is provided.

Standard Five: Permitted Uses and Disclosures of PHI When the SHCC Provides the Patient with the Notice of Privacy Practices. Permitted Uses and Disclosures of PHI by the Self-Funded Health Plan is in Section IV.

- Treatment, Payment and Operations
- Minimum Necessary Standard
- Incidental Uses and Disclosures
- Disclosures for Workers’ Compensation Purposes
- See Standard Six for Uses and Disclosures Requiring Authorization
- See Standards Seven through Ten Describe Other Uses and Disclosures
- 45 C.F.R. 164.502, 164.506, 164.514, 164.530

Permitted Uses and Disclosures that Do Not Require the Individual’s Authorization

So long as the SHCC’s Notice of Privacy Practices includes a description of these practices, the SHCC may use or disclose PHI for the following purposes (if the Notice does not include a description of these practices, then the SHCC must obtain Authorization, even if it would normally be permitted without Authorization):

1. To the individual or to the Department of Health and Human services to investigate compliance with the Privacy Rule, without limitation;

2. For its own treatment, payment and health care operations (TPO) (see the detailed definition for treatment, payment and operations) so long as the SHCC has provided the individual with Notice and made a good faith effort to obtain the individual’s signed Acknowledgment;

27 The PHI consists of findings related to a work-related injury, illness or medical surveillance; the employer needs the information in order to comply with its obligations under 29 CFR parts 1904-1928, 30 CFR parts 50-90.
3. For the treatment activities of any health care provider, including those not covered by the Privacy Rule;

4. To another covered entity or a health care provider (including those not covered by the Privacy Rule) for the payment activities of the entity or provider that receives the PHI;\(^{28}\)

5. To another covered entity for certain health care operations of the entity that receives the information when:
   a) Each entity has or had a relationship with the individual who is the subject of the information and the information pertains to the relationship; and
   b) The disclosures is for those health care operations activities and include quality-related health care operations, teaching activities or for purpose of health care fraud and abuse detection or compliance;

6. With a Limited Data Set or Deidentified Data Set;

7. For psychotherapy treatment by the originator of the psychotherapy notes (all other uses and disclosures require the individual’s Authorization); or

8. For certain functions related to government or public health activities.

**Minimum Necessary Standard. 45 C.F.R. 164.502 and 164.514**

The minimum necessary standard requires the SHCC to evaluate its practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI. The minimum necessary standard does not apply to:

1. Disclosures to or requests by a health care provider for treatment purposes;

2. Disclosures to the individual who is the subject of the information;

3. Uses and disclosures that have been authorized in writing by the individual;

4. Uses and disclosures required for compliance with HIPAA Administrative Simplification Rules;

5. Disclosures to the Department of Health and Human Services (HHS) for Privacy Rule enforcement purposes; or

6. Uses or disclosures that are required by law.

---

\(^{28}\) A physician may send health coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual. A hospital ED or Trauma Unit may give PHI payment information to an ambulance service provider that transported the patient to the hospital so that the ambulance provider can bill.
The covered entity within the SHCC must have a method to categorize and identify the persons or classes of persons who need access to PHI and the categories or types of PHI needed and the conditions appropriate to such access. Except for those purposes where the minimum necessary standard applies, all requests for the entire medical record or Designated Record Set should be justified; otherwise, the request and disclosure by the SHCC may be a violation of the Rule. The SHCC may rely on the presumption that the requested PHI is minimum necessary when a request is from a public official, researchers with appropriate documentation from an Institutional Review Board (IRB), another covered entity or a professional who is a member of the UC workforce or a business associate.

APPLICATION OF THE MINIMUM NECESSARY STANDARD TO THE USE OF PHI FOR TREATMENT PURPOSES

The minimum necessary standard applies to the use of PHI for treatment purposes, with use defined as “the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.” The SHCC has determined that the patient’s health care team, including doctors, nurses, and housestaff may use the individual’s full medical record, without limitation, so that the patient has access to treatment protocols that provide for quality of care and so that the institutional and individual providers can comply with all state and other laws regarding appropriate and timely treatment.

INCIDENTAL USES AND DISCLOSURES

An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule. The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards to protect PHI and has implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure.

The Privacy Rule does not require the SHCC to make structural or systems change, including soundproofing or encryption and does not prohibit such routine practices as patient sign-in sheets at reception areas, X-ray light boards or storage of patient records at bedside. Current practices, such as warning signs in elevators and other public places regarding disclosure of confidential PHI by staff, are consistent with reasonable HIPAA implementation.

An incidental use or disclosure is not permitted if it is a byproduct of a use or disclosure that is a violation of the Privacy Rule. If a DHHS investigation concluded that the disclosure incidental to

---

29 Examples of permissible incidental uses and disclosures: health care staff can discuss the patient’s condition or coordination of treatment services at nursing stations or in semi-private rooms, with the patient, provider or family member; discussion of patient’s condition during training rounds; a pharmacist may discuss a prescription with a patient at the pharmacy counter or over the phone.

30 Examples of reasonable safeguards include: speaking quietly when discussing a patient’s condition in an area where you could be overheard; isolating or locking medical records files and rooms; providing additional password security on computers that maintain PHI; using cubicles or shield-type dividers in areas where multiple patient-staff communications occur. See pages 15 –20 of the OCR HIPAA Privacy Rule Guidance, December 3, 2002 for additional safeguards.
an activity that was a Privacy Rule violation was intended and/or reasonable safeguards did not exist, the SHCC entities and/or workforce members could be subject to substantial sanctions or fines.

WORKER’S COMPENSATION

Workers’ compensation insurers, workers’ compensation administrative agencies and employers are not HIPAA covered entities. Workers’ compensation records that are a part of employment records are not PHI. However, these entities need access to an individual’s health information and PHI maintained by the SHCC. The Privacy Rule allows disclosures to workers’ compensation entities without the individual’s authorization to the extent necessary to comply with laws relating to workers’ compensation, as required by state or other law and for purposes of obtaining payment for any health care provided to the injured or ill worker.

The minimum necessary standard applies to disclosures by the SHCC, except when disclosing PHI as required by state or other law and pursuant to the individual’s authorization.

Individuals do not have a right under the Privacy Rule to request that the SHCC restrict a disclosure of PHI for workers’ compensation purposes when that disclosure is required by law or necessary to comply with workers’ compensation or similar law.

When PHI regarding an injured worker’s previous condition is not directly related to the claims for compensation, the SHCC should obtain the worker’s signed Authorization for that disclosure.

STANDARD FIVE IMPLEMENTATION POLICIES

Implementation Policy 5-1

The SHCC must develop policies and procedures that reasonably limit the use and disclosure of PHI to the minimum necessary standard for payment and health care operations. A failure to apply institutional and individual safeguards that minimize incidental disclosures or to apply the minimum necessary standard when accessing, using or disclosing PHI, is a violation of the Privacy Rule and UC policy.

Implementation Policy 5-2

The SHCC must develop role-based access policies and procedures that limit which members of the workforce have access to PHI for treatment, payment and health care operations, based on those who need access to the information to do their jobs. These policies and procedures should identify the classes of persons within the SHCC who need access to the PHI, (including those who need to access the full medical record or designated record set), the categories or types of PHI needed and conditions appropriate for such access (e.g., security access).

OCR/Privacy Guidance, December 2002, p. 57. If a hospital employee is allowed to have routine, unimpeded access to a patient’s complete DRS or medical record, where such access is not necessary for the employee to do his job, the SHCC has not applied the minimum necessary standard. This is a Privacy Rule violation.
In the absence of systems that offer substantial control over access, the SHCC can implement an attestation system supported by education of the workforce.

**Implementation Policy 5-3**

The SHCC’s patient’s care team, including doctors, nurses, housestaff and other workforce members as determined by the SHCC, may use the individual’s full medical record, without limitation, so that the patient has access to treatment protocols that provide for quality of care and so that the institutional and individual providers can comply with all state and other laws regarding appropriate and timely treatment.

**Implementation Policy 5-4**

The minimum necessary standard applies to the SHCC’s own use of PHI for health care operations, including clinical teaching of health care professionals. For purposes of achieving and sustaining its academic mission, the SHCC allows the use of the individual’s full medical record when such access is necessary to the teaching program and when individuals engaged in those teaching activities have received the SHCC’s HIPAA education program.

**Implementation Policy 5-5**

The minimum necessary standard applies to the health information that may be disclosed as part of payment transactions between health plans and health care providers. When a health plan requests additional information to process a specific claim, in addition to the required and situational elements under the Transactions Rule, the SHCC should be able to rely on the fact that the request by the health plan complies with the Privacy Rule’s minimum necessary requirements. When the entire medical record is requested for payment or operations, the SHCC should document the specific justification for the request and disclosure.

**Implementation Policy 5-6**

When the SHCC receives requests from non-UC covered entities for PHI, the SHCC may rely on the judgment of the requesting covered entity that the entity is requesting only the minimum amount of information that is needed. However, the SHCC has discretion to make its own minimum necessary determination regarding requests from other entities.

When the SHCC receives requests from private, third parties who are not covered entities (e.g., financial institutions or credit card payment systems), the SHCC should make its own determination as to whether the PHI requested is the minimum necessary for the transaction, except when the financial institution is acting as a business associate of the covered entity.

---

32 UC provides health professional training in its Schools of Medicine, Nursing, Dentistry, Optometry, Pharmacy and Public Health.

33 Final Privacy Rule, August 2002, p. 41 of 216.
Implementation Policy 5-7

For disclosure of PHI to a researcher, the SHCC may reasonably rely on documentation of approval of the research protocol or the IRB-approved Waiver of Authorization that the information requested is the minimum necessary for the research purpose.

Implementation Policy 5-8

The SHCC may rely on the judgment of the individual that the PHI requested is the “minimal necessary” if the individual is a public official or agency, another covered entity, a professional member of the SHCC workforce or business associate or a researcher accessing PHI with IRB approval.

Implementation Policy 5-9

The SHCC can disclose PHI to workers’ compensation entities (e.g., Workers’ compensation insurers, workers’ compensation administrative agencies and employers) without the individual’s authorization as follows:

1. To the extent necessary to comply with laws relating to workers’ compensation or similar programs that provide benefits for work-related injuries or illness, including the Black Lung Benefits Act, the Federal Employees’ Compensation Act, the Longshore and Harbor Workers’ Compensation Act, and the Energy Employees’ Occupational Illness Compensation Program Act;

2. To the extent the disclosure is required by state or other law, and the disclosure is limited to what the law requires; and

3. For purposes of obtaining payment for health care provided to the injured or ill worker.

Implementation Policy 5-10

When disclosing information to worker’s compensation entities as required by state or other law, the SHCC does not need to make a minimum necessary standard determination and may reasonably rely on the public official’s representations that the request for a disclosure is the minimum necessary for the intended purpose.

Implementation Policy 5-11

When PHI regarding an injured worker’s previous condition is not directly related to the claims for compensation, the SHCC should obtain the worker’s signed Authorization for that disclosure.

Implementation Policy 5-12

An employee’s health information maintained by UC in employment records for purposes of complying with workers’ compensation laws is not PHI and the employer is not a covered entity. In this case, UC does not have to comply with the Privacy Rule when using or disclosing health information contained in employment records. However, state or other federal law may apply to the confidentiality of that information.
Implementation Policy 5-13

Each SHCC workforce member must be aware of those types of oral or written communications that pose some risk of incidental use or disclosure of PHI. Workforce members must take responsibility for maintaining confidentiality, where reasonably possible, when engaging in activities such as the following:

1. Face-to-face or telephone discussion of a patient’s condition or lab tests with other health care staff and providers, the patient or family members or others involved in the patient’s care;

2. Calling out a patient’s name in a waiting room; and

3. Discussing a patient’s condition during teaching rounds.

Implementation Policy 5-14

The University’s SHCC does not need to include incidental disclosures in an accounting of disclosures.

Implementation Policy 5-15

Within the SHCC, there may be circumstances in which volunteers or contracted individuals have access to PHI that is incidental to their job (e.g., when a cleaning service collects trash, an outside entity takes photos of newborns, or clowns entertain children in the University’s Children’s Hospitals). To provide reasonable safeguards to protect the individual’s PHI that may be incidentally disclosed in these situations:

1. Those outside entities or persons should receive training regarding the Privacy Rule and should sign a confidentiality agreement; and

2. When volunteers carry out these activities, they are SHCC workforce members and must receive the SHCC’s HIPAA training.

Implementation Policy 5-16

When the SHCC engages in non-routine uses and disclosures, the SHCC should establish policies and procedures to provide for a review of those requests for PHI. A supervisory employee or similarly responsible individual must approve these non-routine uses and disclosures.

Standard Six: Uses and Disclosures of PHI That Require an Authorization from the Individual

- Use and Disclosure of Psychotherapy Notes
- Effect Of Prior Authorization
- 45 C.F.R. 164.508, 164.512, 164.514, and 164.532
The SHCC must have written and specific Authorization from an individual for uses and disclosures of PHI, unless the use or disclosure is permitted under the Privacy Rule or required by law. The University’s HIPAA Implementation Packet includes several Authorization forms approved by the Office of the General Counsel for use by the SHCC. A valid Authorization must include an identification of the PHI to be used or disclosed, by whom (name or class of person), to whom, and an expiration date. A research authorization may state as the expiration date: “the end of the study” or “none” if the Authorization is to establish a database for future use. The Authorization must also include the following notifications to the individual:

1. The individual may revoke the Authorization in writing and indicate how to do so;
2. Treatment, payment, enrollment or eligibility for benefits may not be conditioned on an Authorization;
3. PHI may be redisclosed\(^{34}\) by the person receiving PHI, and in that case, the confidentiality of the PHI is no longer protected; and
4. When the Authorization is for marketing purposes, the Authorization must notify the individual of any direct or indirect remuneration to the SHCC from another party.

**PRIOR LEGAL PERMISSIONS**

The SHCC may use consents, authorizations and legal permissions obtained prior to the HIPAA compliance date of April 2003 for treatment, payment, healthcare operations, and for purposes other than to carry out treatment, payment, and health care operations for PHI received or created prior to April 2003.

**AUTHORIZATION FOR USE OR DISCLOSURE OF PSYCHOTHERAPY NOTES**

Authorization is generally needed for use or disclosure of psychotherapy notes even for treatment, payment or operation, except as described in Implementation Policy 6-6.

**STANDARD SIX IMPLEMENTATION POLICIES**

**Implementation Policy 6-1**

The UC model Authorization Form(s) should be used by all SHCC workforce members and entities. The Authorization contains all elements required by the rule and includes the required notifications in plain language. If an Authorization does not contain the required elements or if the information provided to the individual to sign is false (i.e., a deliberate misrepresentation of the

\(^{34}\) In conjunction with the required redisclosure notification to the individual, the authorization may include information about other protections provided to the individual’s PHI. For example, the authorization may state that a drug company sponsor of research is restricted by contract to only use PHI to obtain government approval of the drug under study.
truth), the Authorization is not valid under the privacy Rule. Any use or disclosure of any PHI under those circumstances is a violation of the Privacy Rule.

**Implementation Policy 6-2**

The SHCC must obtain the individual’s signature on the Authorization and provide the individual with a copy of the signed Authorization. When another individual has authority to sign on an individual’s behalf, the SHCC must verify and document that person’s authority to sign such legal permission. The SHCC must document and retain all signed Authorizations for six years, including those provided by a researcher when obtaining PHI for an IRB approved protocol.

**Implementation Policy 6-3**

The SHCC may combine Authorizations, so long as the provision of treatment, payment, enrollment in a health plan or eligibility for benefits is not conditioned on obtaining any of the Authorizations. Authorizations for use or disclosure of psychotherapy notes may be combined only with another Authorization for the use or disclosure of psychotherapy notes. The SHCC may not combine the Authorization with the Notice of Privacy Practices or the written Acknowledgment of that Notice.

**Implementation Policy 6-4**

The SHCC may not require an individual to provide an Authorization to use or disclose his/her PHI for treatment, payment, enrollment in a health plan or eligibility for benefits, except when the treatment is part of a research study that requires the individual’s authorization (see Standard Nine).

**Implementation Policy 6-5**

A patient has a right to revoke or modify an Authorization for use or disclosure of PHI, and the SHCC will be bound by the revoked or modified Authorization from that date forward, except to the extent that the SHCC has taken action in reliance on the Authorization or if the Authorization was obtained as a condition of obtaining insurance coverage and other laws give the insurer the right to contest the claim or policy. The revocation has no effect on actions taken prior to the date of the revocation.

The individual must provide a written request for revocation or modification of the Authorization, and revocations or modifications to the Authorization must be executed within 30 days of receipt of a written request. The SHCC entities should implement local procedures to record and communicate all Authorization modifications or revocations and to make sure the change is noted in the individual’s medical record when appropriate.

**Implementation Policy 6-6**

The SHCC must obtain a signed Authorization for uses and disclosures that are not otherwise permitted by the Privacy Rule or required by law, including the following:

1. Use or disclosure of psychotherapy notes, except:
   a) Use by the originator of the notes for treatment;
b) Use or disclosure by the SHCC of its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling; or

c) Use or disclosure by the SHCC to defend itself in a legal action or other proceeding brought by the individual; and

d) Use or disclosure that is required or permitted with respect to oversight of the originator of the notes.

2. For marketing of PHI to third parties (see Standard Ten), and the Authorization must state whether the SHCC receives any direct or indirect remuneration from the third party. Authorization is not required for:

   a) Communications that are face-to-face between the SHCC and the individual;

   b) Communications that describe the SHCC’s own products or services to an individual; or

   c) Promotional gifts from the SHCC to the individual;

3. IRB-approved research protocol that requires informed consent and the individual’s Authorization;

4. Use of research data that was obtained prior to April 2003:

   a) With an IRB-approved Waiver of Consent, but the IRB has subsequently determined that the protocol post-April 2003 requires informed consent;

   b) For enrollment of new subjects in an ongoing study, which was approved prior to April 14, 2003 and requires Informed Consent;

5. Disclosure of PHI to the patient’s employee (including those situations when the patient is a UC employee and the disclosure is to UC), except:

   a) When the use and disclosure is for public health activities;

   b) To conduct an evaluation relating to medical surveillance of the workplace; or

   c) To evaluate whether the individual has a work-related illness or injury.

---

35 The researcher can seek approval to use deidentified data or a limited data set without patient Authorization or IRB approved Waiver of Authorization. See Standard Nine.

36 The PHI that is disclosed to the employer must consist of findings concerning the work-related illness, or injury or to comply with federal law or similar state law. The SHCC must provide written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer. The Notice can be provided at the time of health care delivery or by posting the Notice at the site of delivery.
6. Use of a list for fundraising activities that has been created using disease or treatment PHI or that clearly identifies an individual and his/her specific disease or treatment;

7. Use and Disclosure of PHI to the media or through other forms of external communications;

8. Use or creation of disease or treatment specific data bases (data bases that have not been deidentified or with limited data sets) for purposes including fundraising, continuing medical education (CME) courses, other teaching activities that are not a part of the SHCC’s own teaching functions, research that requires the individual’s informed consent, fundraising activities;

9. Use of disease or treatment specific data bases (that are not deidentified or limited data sets) created prior to April 2003 if those data bases were not created with specific legal permission from the individuals whose PHI is included in the data base;  

10. The SHCC may not disclose PHI to another covered entity without authorization or the use of a Limited or Deidentified Data Set (LEGAL) for the following operational activities of the other entity: resolution of internal grievances, customer service, medical review or auditing activities; or

11. In the cases of State civil subpoenas, the SHCC must be served either with the patient’s Authorization or a Notice to Consumers, along with the subpoena. For judicial and administrative proceedings in response to a court order, subpoena, discovery request or other lawful process, the SHCC should make sure that the requesting entity provides an Authorization or has made reasonable efforts to notify the patient of such disclosure, has allowed time for the patient to object, that the patient has Authorized or the court has resolved the issue through issuance of an appropriate order including a protective order. Seek the advice of the Office of the General Counsel when it is not clear if an Authorization is required. The PHI should be returned or destroyed on completion of its use by the court or other requesting entity;

12. The SHCC must obtain Authorization or use a deidentified data set when disclosing PHI to an OPO for purposes other than the purpose of facilitating organ, eye or tissue donation and transplantation;  

---

37 The Privacy Rule does not “grandfather” preexisting databases unless express legal permissions was obtained from the individual and the permission applies to the intended use or disclosure. Pre-April 2003 research, fundraising, media, and personal data bases that contain disease or treatment specific information require the patient’s Authorization for use or disclosure of the PHI.

38 The Privacy Rule requires the SHCC to make sure that the requesting entity has made an effort to notify the patient of such disclosure, has allowed time for the patient to object, that the patient has agreed or the court has resolved the issue through issuance of an appropriate order including a protective order. However, in some cases California Law requires notice to the individual, not just “an effort.”

39 For example, for purposes of disclosing to the organ donor information about the recipient’s health status and OPO staff participation in the transplant or harvesting surgery.
13. When PHI regarding an injured worker’s previous condition is not directly related to the claims for compensation.

**Implementation Policy 6-7**

Each member of the SHCC’s workforce is responsible for understanding the requirements for using and disclosing PHI if, in the course and scope of employment, s/he may be required to use or disclose PHI. In all cases when a SHCC workforce member is not certain whether or not an Authorization is required or is seeking to use or disclose PHI that is not permitted or required by law, s/he must consult with the University Privacy Official, campus Privacy Officer or the Office of the General Counsel prior to using or disclosing that information or requesting that the patient sign an Authorization.

**Standard Seven: Uses and Disclosure of PHI to Other Covered and Non-Covered Entities**

- Treatment
- Payment
- Operations
- Teaching Activities
- Organized Health Care Arrangement (OHCA) and Affiliated Covered Entities
- 45 C.F.R. 164.501, 164.504, 164.506, 164.514

The SHCC frequently exchanges PHI with outside HIPAA-covered or non-covered entities in order to carryout the mission of education, patient care/service, and research. The Privacy Rule has not anticipated all such exchanges that may occur in an organization such as UC that is a hybrid covered entity with multiple covered functions and a tripartite mission. In order to provide workability of the Privacy Rule and maintain the flexibility needed to sustain the mission and comply with the Privacy Rule, the HIPAA Taskforce has endeavored to interpret the requirements of the Privacy Rule and develop policies and procedures that both support the principles of the Privacy Rule and continue to allow the SHCC to provide access to quality care, education of the healthcare workforce and leading edge research. Standard Seven includes Implementation Policies that are the result of considerable policy analysis and legal review by the HIPAA Taskforce of the Privacy Rule, the Preamble, and subsequent guidance from the Office for Civil Rights.

**Treatment Purposes of Another Entity**

When a patient is referred for treatment from the University’s SHCC to another covered or non-covered health care provider (or when a patient is referred to the SHCC from another covered or non-covered health care provider), PHI can be disclosed without need for a HIPAA Authorization. The Privacy Rule also states that no business associate agreement is required when two providers exchange PHI for treatment purposes. For example, a physician does not need to obtain a patient’s written Authorization to send a copy of the patient’s medical record to a specialist or other health
care provider who is not part of the SHCC. The SHCC does not need to apply the minimum necessary standard to disclosure to or requests by a health care provider for treatment purposes.

**PAYMENT PURPOSES OF ANOTHER ENTITY**

The SHCC may disclose PHI to another covered entity (provider, plan or clearinghouse) or non-covered health care provider for the payment purposes of the other entity, including uses and disclosures necessary for coordination of benefits. The SHCC must apply the minimum necessary standard to all such disclosures. The SHCC cannot disclose PHI to any other non-covered entity for the payment purposes of that entity.

**ORGANIZED HEALTH CARE ARRANGEMENT**

Separate covered entities may share PHI if they are parts of an Organized Health Care Arrangement (OHCA). Covered entities must formally agree to participate in an OHCA and may, but are not required to, use a joint Notice of Privacy Practices and Acknowledgement to use and disclose PHI for the purposes of joint treatment, payment, and health care operations. If separate notices are used, each should identify the OHCA and sharing of PHI. To establish such an OHCA, the entities must be integrated clinically or operationally and the PHI that is shared must be used for joint management or operational purposes.

To qualify as an OHCA, the covered entities must:

1. Hold themselves out to the public as participating in a joint arrangement; and
2. Participate in at least one of these joint activities:
   a) Utilization review;
   b) Quality assessment; or
   c) Payment activities.

A teaching relationship alone does not qualify covered entities to be considered an OHCA. As of April 14, 2003, the UC SHCC is not participating in any OHCA arrangements.

**AFFILIATED COVERED ENTITIES**

Covered entities that share governance or ownership (5% or more) may designate themselves as Affiliated Covered Entities (ACE) and share PHI. They may, but are not required to, utilize a single Notice of Privacy Practices, single privacy program and privacy officer. The Notice of Privacy Practices must indicate the existence of the ACE and sharing of PHI. The terms of authorizations, restrictions and recisions of authorizations and requests for records access, amendments and accounting of disclosures affect all affiliates.

A teaching relationship alone does not qualify covered entities to be considered affiliates. As of April 14, 2003, the UC SHCC is not participating in affiliated covered entity arrangements, as defined under HIPAA. However, all UC academic health centers engage in affiliated relationships with other teaching institutions for purposes of carrying out their graduate medical education and other teaching requirements as accredited teaching organizations.
**BETWEEN GOVERNMENTAL INSTITUTIONS**

In those instances where the SHCC or other governmental entities have a business associate type relationship, the SHCC can comply with the requirements of a Business Associate Agreement by entering into a Memorandum of Understanding with the other entity. A relationship that is for treatment purposes does not require a Business Associate Agreement. The SHCC should consult with the local or University Privacy Official or Office of the General Counsel to ascertain that the relationship is that of a business associate.

**STANDARD SEVEN: IMPLEMENTATION POLICIES**

**Implementation Policy 7-1**

Treatment Purposes: When the SHCC refers a patient for treatment to another covered or non-covered health care provider, the SHCC can disclose PHI for treatment purposes, and the minimum necessary standard does not apply. No Authorization or Business Associate Agreement is required.

**Implementation Policy 7-2**

Payment Purposes: The SHCC may disclose PHI to or receive PHI from another covered provider, covered entity or non-covered health care provider for the payment purposes of that entity, including uses and disclosures necessary for coordination of benefits. The SHCC must apply the minimum necessary standard to all such disclosures. No Authorization or Business Associate Agreement is required.

**Implementation Policy 7-3**

Operations of Another HIPAA-Covered Entity. The SHCC may disclose PHI to another covered entity for the health care operations of the covered entity or to the SHCC’s business associate under the following limitations:

1. Each entity has or had a relationship with the individual who is the subject of the information;

2. The PHI exchanged pertains to that relationship;

3. The purpose is for operations that include: 40 quality assessment and improvement activities; population-based activities relating to improving health or reducing health care costs; case management and care coordination; certification; conducting training programs; accreditation; certification; licensing or credentialing activities; health care fraud and abuse detection or compliance.

40 Only for purposes listed in 45 CFR 164.501, paragraphs (1) and (2) of the definition of health care operations in the Privacy Rule.
**Implementation Policy 7-4**

Teaching Operations of Both Covered Entities: When the SHCC’s covered health care providers have a teaching relationship with another covered entity and the covered entity’s patients under a UC teaching affiliation agreement or other legal agreement that describes the teaching relationship, the covered entities may share PHI regarding the individual so long as:

1. Both covered entities have a teaching relationship with the individual;
2. The SHCC’s Notice provides Notice of the use and disclosure of PHI for teaching activities; and
3. The minimum necessary standard applies.

**Implementation Policy 7-5**

Other Operations of a HIPAA-Covered Entity: The SHCC must use an Authorization, LDS or Deidentified data set to disclose PHI to another covered entity for the following operational activities of the other entity: resolution of internal grievances, customer service, medical review or auditing activities.

**Implementation Policy 7-6**

Operations of a Non-HIPAA Covered Entity: The SHCC must obtain Authorization or use a LDS deidentified data to disclose PHI to a non-HIPAA Covered Entity for all operations of that entity.

When the disclosure is for teaching purposes and is to a trainee whose sponsoring institution is not a HIPAA-covered entity (e.g., and allied health professionals program at a state college), the SHCC may disclose a Deidentified Data Set or enter into a Data Use Agreement with the non-covered entity and allow the disclosure of a Limited Data Set. The SHCC may enter into a Business Associate Agreement with the recipient of the Deidentified or Limited Data Set data (e.g., the student or institution) that allows the recipient to act as a Business Associate of the SHCC in order to create the Deidentified or Limited Data Set. The Business Associate Agreement can be combined with the Data Use Agreement.

**Implementation Policy 7-7**

In many teaching situations, particularly Continuing Medical Education Programs (CME), SHCC providers and faculty will disclose health information for non-SHCC teaching activities and, in

---

41 There is no definition in the Privacy Rule for the term “relationship.” The SHCC has interpreted relationship to include a teaching relationship that both covered entities have to the patient as demonstrated in an affiliation agreement or other legal document entered into between the two covered entities.

42 Trainees include those students who, in the course of their educational experience will be a part of the SHCC workforce; have a teaching relationship to patients within the SHCC; are from sponsoring teaching organizations that are not covered entities; and as a requirement of their sponsoring organization’s educational experience must use patient health information to complete their coursework.
most cases, the information will be disclosed to individuals who have no teaching relationship to
the patient whose health information is being disclosed (see Implementation Policy 7-4). For all
such purposes, the SHCC workforce member must:

1. Obtain a signed Authorization from the individual whose PHI would be the subject of the
disclosure. If the SHCC’s workforce member receives remuneration as a result of the use
and disclosure of PHI for these purposes, the Authorization must state that fact to the
individual; or

2. Create a Limited Data Set and enter into the SHCC’s Confidentiality Agreement/Data Use
Agreement⁴³; or

3. Create a deidentified data set that removes all 18 personal identifiers.

Implementation Policy 7-9

When a member of the workforce is uncertain as to when an Authorization is required prior to
disclosing PHI, he/she must consult with either the campus Health Information Management
Service, HIPAA Privacy Officer, University HIPAA Privacy Official or the Office of the General
Counsel.

Standard Eight: Use and Disclosure Required by Law, Public Health or Judicial
and Law Enforcement Proceedings and for Specialized Government Functions.
45 C.F.R. 164.512

As with other Standards within the System Standards, Standard Eight may be modified based on
ongoing legal review and analysis of state law. When state law provides greater protection for an
individual’s health information, enhanced patient rights or access to an individual’s health
information, state law is “more stringent” and preempts the Privacy Rule. When a member of the
UC SHCC workforce is not certain as to what is required under state law or when state law
provides greater protections to the patient or individual, the UC workforce member must seek
advice from the Office of the General Counsel.

ACCOUNTING FOR DISCLOSURES

In general, the individual must receive an accounting of all disclosures required or permitted
under this section if the individual makes that request in writing to the designated SHCC
individual or department because these are uses and disclosures for which an authorization or

opportunity to agree or object is not required under the Privacy Rule. See exceptions under Implementation Policy 8-5.

USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED UNDER THE PRIVACY RULE

The SHCC may use or disclose PHI to the extent permitted or required by law as follows:

1. For disclosures about victims of abuse, neglect or domestic violence; In the case of disclosures related to abuse, neglect or violence, the patient must be notified of the disclosure unless this may harm the patient;

2. For public health activities to prevent or control disease, injury or disability, adverse drug or product defects or product recalls, report quality or safety or effectiveness of Food and Drug Administration (FDA) regulated activities or products;

3. To an employer for the purposes of workplace medical surveillance or to report a work-related illness or injury if the SHCC provides written Notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer. When occupational health clinics provide these functions on the worksite of the employer, the Notice must be provided at time the care is provided or by posting the Notice in a prominent place where the care is provided;

4. To a Health Oversight Agency (see definition) for health oversight activities authorized by law, such as audits, investigations, licensure, and disciplinary actions or for oversight of the health care system, government benefits programs, compliance with program standards, enforcement of civil rights laws;

5. In the cases of State civil subpoenas, the SHCC must be served either with the patient’s Authorization or a Notice to Consumers, along with the subpoena. For judicial and administrative proceedings in response to a court order, subpoena, discovery request or other lawful process, the SHCC should make sure that the requesting entity provides an Authorization or has made reasonable efforts to notify the patient of such disclosure, has allowed time for the patient to object, that the patient has Authorized or the court has resolved the issue through issuance of an appropriate order including a protective order. Seek the advice of the Office of the General Counsel when it is not clear if an Authorization is required. The PHI should be returned or destroyed on completion of its use by the court or other requesting entity;

6. For law enforcement purposes to a law enforcement official, when required by law or in compliance with a court order/warrant or an administrative request or summons. The

---

44 The PHI consists of findings related to a work-related injury, illness or medical surveillance; the employer needs the information in order to comply with its obligations under 29 CFR parts 1904-1928, 30 CFR parts 50-90.

45 the Privacy Rule requires the SHCC to make sure that the requesting entity has made an effort to notify the patient of such disclosure, has allowed time for the patient to object, that the patient has agreed or the court has resolved the issue through issuance of an appropriate order including a protective order. However, in some cases California Law requires notice to the individual, not just “an effort.”
information sought must be relevant and material to the law enforcement and it needs to be specific and limited in size to the extent practicable. If the request pertains to a suspect, fugitive, material witness or missing person, the PHI that can be released is limited to demographic data, name and address, date and place of birth, blood type, type of injury, date of treatment or death, physical disabilities to identify the patient. Disclosures of PHI may be made to law enforcement if it pertains to an individual who is suspected to be or is a victim of a crime;

7. The SHCC may disclose PHI to law enforcement personnel about the death of an individual if a crime occurs on the premises of the covered entity and in response to a medical emergency not on the premises of the covered entity;

8. To coroners, medical examiners and funeral directors for the purpose of identifying a deceased person, determining the cause of death or as otherwise required by law;

9. The SHCC may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation;

10. To persons reasonably able to prevent or lessen the serous threat to public health or safety; or

11. For specialized government functions, including military personnel, veterans, foreign military personnel and national security activities;\(^{46}\)

STANDARD EIGHT IMPLEMENTATION POLICIES

Implementation Policy 8-1

All requests for disclosures under this Standard must be directed to individuals with expertise and authority to determine what is permitted under HIPAA and State Law, including the Office of the General Counsel, local or system Privacy Officers, Health Information Management or Medical Record Services.

Implementation Policy 8-2

The SHCC may use or disclose PHI to the extent required or permitted by law. In most cases, the Privacy Rule requires the SHCC to obtain and document reasonable assurances (See Standard Documentation) that an individual or entity that is requesting PHI is permitted or required by law to receive the PHI. The SHCC may reasonably rely on documentation or statements provided by the requestor, so long as the SHCC receives verification of the individual’s authority as required under the Privacy Rule, including representation from a public official, the presentation of official

\(^{46}\) Specialized government functions include those that may be dictated by appropriate command authorities, in relation to national security activities as authorized by the National Security Act, the USA PATRIOT Act, to federal officials authorized to protect the President or other officials, in response to security clearance activities, correctional institutions and other law enforcement custodial situations, and covered entities that are government programs providing public benefits. Additionally, these regulations address disclosures within the Department of Veteran Affairs.
identification, a written request on official letterhead or a warrant, subpoena, order or other legal process.

**Implementation Policy 8-3**

When PHI is released without patient Authorization to a legal authority, the SHCC must provide a cover letter with the material to serve as a reminder to the recipients that the PHI is of a sensitive nature and must be handled as such and destroyed when no longer needed.

**Implementation Policy 8-4**

If the disclosure is related to a report of abuse, neglect or domestic violence, use the official report form (sample in Appendix A), which indicates when the patient or representative should not be notified. Use a special form to supply required PHI to identify or locate a suspect, fugitive, material witness or missing person. In reference to the latter types of disclosures, information about DNA, dental records or typing or analysis of body fluids cannot be released.

**Implementation Policy 8-5**

The SHCC must provide an accounting of disclosures under this Standard, except when the disclosure is for national security purposes, to correctional institutions or for law enforcement custodial purposes or when there is a request for temporary suspension of accounting. If the individual has provided an Authorization for disclosure, no accounting is required.

In responding to a judicial or administrative request for PHI, the entity within the SHCC may elect to notify the patient of the request. If this occurs, the disclosure need not be included in an accounting.

**Standard Nine: Uses And Disclosures For Research**

- Research-related Health Information and the Relationship of Research to the University’s Single Health Care Component
- Research Use/Disclosure Without Authorization/Waiver of Authorization
- Research Authorization
- Limited Data Set and Data Use Agreement
- Deidentified Data
- Research Database, including Organ and Tissue Banks
- Clinical Labs that Participate in Research
- Transition Provisions
- C.F.R. 164.508, 164.510, 164.512, 164.528 and 164.530
IMPACT OF HIPAA/THE PRIVACY RULE ON RESEARCH

The HIPAA Privacy Rule applies to three types of covered entities—health care providers, health plans, and health care clearinghouses. The Rule requires covered entities to implement policies and procedures that provide for the privacy and security of an individual’s health information when that Protected Health Information (PHI) is used, disclosed or created by one or more of the covered entities. With a few exceptions, the Privacy Rule allows covered entities to use or disclose PHI for treatment, payment and operations without the patient’s Authorization, but requires Authorization by the patient for most other activities. Research is not considered to be treatment, payment or operations. Section 164.508 of the Privacy Rule, however, states that PHI may be used or disclosed for purposes of research, and that research may create PHI de novo. The Privacy Rule specifies that research uses of PHI must be reviewed and approved either by a duly constituted Institutional Review Board (IRB) or by a Privacy Board whose membership meets the requirements outlined in the Privacy Rule. The Privacy Rule also contains specific review criteria for approval of research uses of PHI without Authorization (i.e., without obtaining consent from the individual whose data are being used for research), and it contains documentation requirements when signed Authorizations for research uses of PHI are obtained. Because Privacy Rule requirements apply only to PHI, it is important to understand what information is and is not PHI in a research context.

RESEARCH-RELATED HEALTH INFORMATION (RHI) and the RELATIONSHIP OF RESEARCH TO THE UNIVERSITY’S SINGLE HEALTH CARE COMPONENT (SHCC)

For purposes of compliance with HIPAA, the Regents have designated all covered entities within the University of California as a Single Health Care Component (SHCC) and have supported the recommendation of the University’s HIPAA Taskforce that, in order to reduce costs of compliance and enhance effectiveness, the Taskforce will provide all entities in the SHCC with the materials required for compliance with the Privacy Rule (see Introduction and Standard One). The University’s Single Health Care Component consists of all UC entities covered by HIPAA – five academic health centers, faculty practice plans, student health services at all campuses, federal Department of Energy labs, self-insured health plans, some athletic departments and occupational health centers, and individuals who provide business and finance services to the health plans and the healthcare providers.

A member of the University’s workforce who is both a health care provider and a researcher can be both a covered and a non-covered individual for purposes of complying with HIPAA. A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. (See 45 CFR 160.102, 160.103). For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and who transmits health information in electronic form to a third party for payment, would be both a covered health care provider and a researcher under the Privacy Rule.48

47 “Research-Related Health Information (RHI) and its Relation to HIPAA Protected Health Information.” Masys D., Mittman C., Robinson A., Jaffe R., Faer M., UC HIPAA Task Force, November 2002.

The University of California’s HIPAA Task Force has coined the term “Research-related Health Information” (RHI) to clarify the types of data used in research that would be person-identifiable but would not be considered PHI. RHI shares some characteristics with HIPAA PHI, but the key distinction between RHI and PHI is that PHI is associated with or derived from a healthcare service event—either the provision of care or payment for care. Research studies that use medical records as a source of personally-identifiable research data are using PHI obtained from a covered entity, and in order to obtain the PHI from a covered health care provider, the researcher must comply with the requirements of HIPAA and obtain IRB or Privacy Board approval. A researcher engaged in interventional clinical studies where treatments are being compared for safety and effectiveness in a setting where services are billed to insurers would create PHI as a product of the research and, in order to participate in such treatments, the patient must provide the required signed consents and Authorizations. All such PHI should be included as a part of the individual’s medical record or HIPAA-defined Designated Record Set maintained by the SHCC and protected as required by the individual or institutional providers covered by HIPAA.

In contrast, a research study that does not include a diagnostic or therapeutic intervention and that does not acquire health-related facts about a person or PHI from the SHCC or its individual providers would create information that, if individually identifiable, would be considered RHI, not PHI. An example of this would be a study of brain imaging in schizophrenia designed to correlate imaging patterns with participant symptoms, where appropriately-consented participants might provide facts about their medical history by interview or by filling out research data forms. Since these data were provided as part of voluntary participation in a study, and not as a byproduct of a healthcare service event, they would be governed by the principles of respect for persons enumerated in the federal Common Rule (45 CFR 46), including the maintenance of confidentiality and security of the information. These data would not be governed by the HIPAA Privacy Rule because they are not PHI, i.e., health information used, disclosed, received or created by an entity covered by the Privacy Rule. Accordingly, these data would not be subject to the Privacy Rule’s administrative requirements for logging of disclosures, business partner agreements, audit trails and the right to request amendment of records.

The concept of RHI recognizes that the Privacy Rule applies to those records associated with an individual’s health care, and that, in some instances, health care records may be used or produced in the course of doing research. RHI defines a related but distinct class of information arising from biomedical and behavioral research that is not associated with health care service provided in a part of the organization that bills for care to an individual, for which there are similar principles of confidentiality but fewer administrative and documentation requirements. When RHI and PHI are admixed in a research project, it may become impossible to determine the source and use of a particular item of information or data. In these situations, the researcher should apply PHI Privacy Standards to any project where even a fraction of the research records are derived from or include PHI.

A member of the UC workforce may serve dual roles as both a covered provider under the Privacy Rule and as a non-covered researcher. A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, in a part of the organization that bills for care.49 The individual researcher has a responsibility to understand

49 OCR HIPAA Privacy Guidance, December 2002.
when his or her activities are covered functions (e.g., as a health care provider) that use, create or disclose PHI and, as such, the provider/researcher must comply with all the requirements of the Privacy Rule and the System Standards. Research is not a covered function and, therefore, the disclosure of PHI to a researcher does not require a business associate agreement. 50

**STANDARD NINE IMPLEMENTATION POLICIES**

**General Requirements for a Researcher to Receive Protected Health Information from The Single Health Care Component (SHCC) or from Other Covered Entities for Research Purposes**

**Implementation Policy 9-1**

If a University researcher wants to obtain an individual’s Protected Health Information (PHI)51 from the University’s Single Health Care Component (SHCC) which includes the covered health care provider (institution or entity) or covered health plan, the researcher must follow current University policy for IRB review and approval and either:

1. Provide the SHCC with a copy of the IRB’s approval for consented research and copies of all signed HIPAA Authorization forms52; or
2. Provide the SHCC with a copy of the IRB’s certification that the research meets the elements of a Waiver of Authorization; or
3. Provide the SHCC with the IRB’s approval for research using a Limited Data Set53; for purposes of creating the Limited Data Set, the SHCC allows the researcher to act as a

50 Preamble to the Final Rule, August 2002. “Disclosures from a covered entity to a researcher for research purposes as permitted by the Rule do not require a business associate contract. This remains true even in those instances where the covered entity has hired the researcher to perform research on the covered entity’s own behalf because research is not a covered function or activity…. Research recruitment is neither a marketing nor a health care operations activity…Only a component that performs covered function may be included in the health care component.”

51 See Standard Two for detailed discussion of PHI. In general, PHI is an individual’s health information that is created, received, used or disclosed by a covered health care provider or health plan and relates to the past, present and future health and health care of the individual or payment for health care provided to the individual.

52 HIPAA mandates that a patient’s signed Authorization include specific elements. See Appendix B for University-approved Authorization forms. The HIPAA-required Authorization may be combined with the Informed Consent.

53 The HIPAA defined Limited Data Set removes direct identifiers of the individual, relatives, employers or household members, including names; postal, IP and email addresses; phone and fax numbers; Social Security and Medical record health plan beneficiary, license and account numbers; device identifiers and serial numbers; URLs; biometric and full face identifiers.
member54 of the SHCC workforce to create the Limited Data Set; the UC researcher, who is the recipient of the LDS, must either sign the UC Confidentiality Agreement or enter into a Data Use Agreement with the SHCC (see Standard Two); or

4. Provide the SHCC with the IRB’s approval letter that allows for research using a de-identified data set and, as in #3 above, allow the researcher to create the de-identified data set in the capacity of a SHCC workforce member providing business services to the SHCC; or

5. Provide the SHCC and/or other covered entities evidence that the requirements for work preparatory to research or for decedent research have been met.

In all cases, except the Limited (#3 above) and Deidentified Data Set (#4 above), assure that only the minimum necessary information is requested and that any PHI created de novo in the course of the research is entered into the medical record or Designated Record Set. The original signed Authorization is kept by the SHCC; a copy of the Authorization may be kept in the research file.

**DISCLOSURE OF PHI FOR RESEARCH PURPOSES WITH THE INDIVIDUAL’S SIGNED RESEARCH AUTHORIZATION**

**Implementation Policy 9-2**

When the IRB has approved a research protocol that requires the subject’s consent to participate in research and in which PHI will be used, HIPAA requires the researcher to provide the subject’s signed Authorization to the covered entity in order to obtain the PHI. The University’s IRBs have developed a Research Authorization Form that meets all the requirements of the Privacy Rule.

During the transition period, the period in which IRB-approved protocols using PHI come into complete compliance with the Privacy Rule and is no later than April 2004, the Research Authorization is attached to the Informed Consent Form (ICF).

The Research Authorization does not have to include an expiration date for research purposes, or for the creation and maintenance of a research database or repository. However, if there is no expiration date, the Authorization must say so.

When providing the researcher with the PHI described in the Authorization, the SHCC must be able to reasonably rely on the assurance that the PHI requested is the minimum information necessary to carry out the research. A researcher may condition the subject’s enrollment in a research study on obtaining the subject’s Authorization for the use of preexisting PHI.

**Implementation Policy 9-3**

California law requires that the Authorization must be “clearly separate from any other language present on the same page and …executed by a signature which serves no other purpose than to

---

54 When a University workforce member provides business services to the SHCC, that individual is considered a part of the SHCC and may use or disclose PHI for those business purposes. In this case, the researcher is providing a service for the SHCC—the service of creating a Limited Data Set—that the SHCC would otherwise have to perform or hire a business associate to perform.
execute the Authorization.55 This requirement may be met by appending a separate Authorization form to the informed consent form, or by inserting Authorization language into the consent form so long as the subject signs the embedded Authorization language in addition to the Consent Form and so long as information regarding the use and disclosure of PHI is clearly separate from all other Consent elements.

**Implementation Policy 9-4**

If a researcher wants to enroll a new participant in a protocol approved by the IRB prior to the Privacy Rule compliance date of April 2003 and if the protocol requires the subject’s consent, HIPAA requires that the subject also sign the HIPAA Research Authorization. Unlike the Common Rule, the Privacy Rule does not require IRBs to review research uses and disclosures made with individual authorization, and in this case, the researcher may obtain the individual’s Authorization and Consent at the same time. If the researcher uses a combined Consent/Authorization Form rather than the stand-alone Authorization form for the transition period, s/he must obtain IRB re-approval of the protocol because this constitutes an amendment to the ICF.

**Implementation Policy 9-5**

The SHCC does not have to provide an accounting to the subject of the uses and disclosures of the individual’s PHI made pursuant to a Research Authorization, but the SHCC must retain all original signed Research Authorizations for six years.

**Implementation Policy 9-6**

A separate Authorization is not required for research that includes treatment, but it may be advisable for the Authorization to include a statement regarding how PHI obtained for a research study will be used and disclosed for treatment, payment or operations, if it will assist the individual in making an informed decision about signing the Authorization.

**Implementation Policy 9-7**

An individual can revoke his or her Authorization for research. The SHCC can continue to use and disclose PHI obtained prior to Authorization revocation as necessary to maintain the integrity of the research study and to the extent that the SHCC has acted on the Authorization. This reliance exception, however, does not permit the SHCC to continue to disclose PHI to a researcher or for its own research purposes if the information was not previously collected at the time the subject withdrew his or her Authorization.

**DISCLOSURE OF PHI FOR RESEARCH PURPOSES THAT DO NOT REQUIRE AN INDIVIDUAL’S AUTHORIZATION**

The SHCC may disclose PHI to a researcher without patient Authorization as follows:

1. IRB or Privacy Board approved and certified Waiver of Authorization; or

55 Assembly Bill No. 2191, an amendment to the Confidentiality of Medical Information Act, Civil Code Section 56.11.
2. IRB or Privacy Board approved protocol using a **Limited Data Set** and with a Data Use Agreement between the researcher and SHCC; or

3. IRB Approved **Preparation** of a Research Protocol; or

4. Research on PHI of **Decedents**; or

5. IRB or Privacy Board approved protocol using **De-identified Data**; or

6. For purposes allowed under law such as notification of adverse events.\(^{56}\)

The Minimum Necessary Standard applies to the request for and disclosure of PHI in these circumstances.

**Implementation Policy 9-8: Waiver of Authorization**

To use or disclose PHI with an IRB or Privacy Board approved Waiver of the individual’s Authorization, the SHCC must receive from the researcher requesting the disclosure of PHI an Institutional Review Board (IRB) Letter of Approval that certifies all of the following:

1. Identification of the IRB and the date on which the Waiver of Authorization was approved;

2. A brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board\(^{57}\);

3. A statement that the Waiver of Authorization has been reviewed and approved under either normal or expedited review procedures as required under the Common Rule; an expedited review process permits the SHCC to accept an IRB’s documentation of Waiver of Authorization when only one member of the IRB has conducted the review.\(^{58}\)

4. The signature of the chair or other member, as designated by the IRB chair, that certifies the Waiver of Authorization; and

5. A statement that the IRB has determined that the Waiver of Authorization, in whole or in part, satisfies the three waiver criteria in the Privacy Rule:

   a) The use or disclosure of PHI involves no more that a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

      i. An adequate plan to protect the identifiers from improper use and disclosure;

---

\(^{56}\) See Section 164.512 (b)(1)(iii) of the Privacy Rule.

\(^{57}\) The researcher is responsible for submitting the description of the PHI to the IRB as a part of the approval process, and the IRB will attach the list of PHI requested to the Letter of Approval.

\(^{58}\) OCR Privacy Rule Guidance, December 2002, p. 92.
ii. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; \(^{59,60}\) and

iii. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this subpart;

b) The research could not practicably be conducted without the waiver or alteration; and

c) The research could not practicably be conducted without access to and use of the PHI.

**Implementation Policy 9-9**

The IRB must document and retain copies for six years of all information that demonstrates that the Waiver of Authorization criteria were met. The SHCC must document and retain for six years copies of all IRB Letters of Approval certifying Waiver of Authorization. The SHCC must provide an accounting to the subject of any disclosures of PHI provided with a Waiver of Authorization.

**Implementation Policy 9-10: Preparation of a Research Protocol**

The University of California takes the position that accessing PHI preparatory to research constitutes human subject research activity and that such activity must be reviewed and approved or exempted by an authorized IRB. \(^{61}\)

In order for the SHCC to allow a researcher access to PHI to prepare a research protocol, the researcher must provide to the SHCC written representation in the form of an IRB approval or exempt registration letter that the following criteria are met:

1. The researcher will not remove any PHI from the SHCC; and

---

\(^{59}\) The Privacy Rule is intended to supplement and build upon the human subject protections already afforded by the Common Rule and FDA’s human subject protection regulations. The Common Rule requires that an IRB must determine that “when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.”

\(^{60}\) The Final Rule Preamble, 114 of 216, “Requiring the researcher to justify the need to retain patient identifiers provides needed flexibility for research, while maintaining the goal of protecting individuals’ privacy interests.”

\(^{61}\) The University of California’s position that research preparatory to research requires IRB review is based on federal regulations at 45CFR Part 46.102 which define “human subject research.”
2. The use or disclosure of the PHI is permitted by the IRB as an activity described in an IRB approved or exempted research protocol (format to be determined by local IRB).

Implementation Policy 9-11: Research Recruitment

The health care providers in the SHCC may discuss with a UC patient the possibility of enrolling in a research protocol as follows:

1. The patient’s SHCC physician may recruit the individual for an IRB-approved research protocol (both therapeutic and non-therapeutic), but must obtain the subject’s Authorization for disclosure of PHI for research purposes even if the patient’s physician is also the researcher; or

2. A researcher who is a member of the SHCC workforce (i.e., a physician or other covered health care provider) or a researcher who is not part of the SHCC (this may include UC faculty who are not part of the SHCC and who are non-covered health care providers) must either ask a covered provider to make the contract with the prospective subject or, in collaboration with a UC Principal Investigator, seek an IRB Waiver of Authorization to obtain the individual’s contact information. The IRB can waive Authorization for this purpose, even if the research protocol requires the individual’s Authorization to participate. In most cases, the primary care provider of the potential research subject will be the preferred advocate for the subject’s interests, and will be the preferred contact point for communications with the subject concerning recruitment for research studies.

Implementation Policy 9-12

The SHCC may disclose decedent PHI to a researcher without an IRB-approved protocol so long as the SHCC receives from the researcher written representation that:

1. The use or disclosure is solely for research on the PHI; and

2. The PHI is necessary for the research.

Implementation Policy 9-13

The Privacy Rule allows an IRB to use expedited review procedures as permitted by the Common Rule to review and approve requests for Waiver of Authorizations or when the research involves no more than a minimal privacy risk to the individuals.

ACCOUNTING FOR DISCLOSURE OF PHI FOR RESEARCH PURPOSES

Implementation Policy 9-14

If requested by an individual whose PHI has been disclosed for research purposes, the SHCC must provide an accounting of those disclosures as follows:

1. Disclosures of PHI made with a Waiver of Authorization;

2. Disclosures of PHI for review preparatory to research; and
3. Disclosures of PHI for decedent research when requested by the decedent’s personal representative.

For studies accessing PHI that involve more than 50 individuals, the SHCC may meet this requirement by providing the individual with a list of all protocols for which the individual’s PHI may have been disclosed, the researchers’ name(s) and contact information, the purpose of the study, the type of PHI sought, and the timeframe of disclosures. When requested, the SHCC must assist the individual in contacting researchers who have accessed their PHI.

**RETROSPECTIVE RESEARCH STUDIES INVOLVING DATA RE-ANALYSIS**

**Implementation Policy 9-15**

When a researcher requests PHI from the SHCC or wants to use data already held by the researcher for purposes of retrospective research studies involving data re-analysis, the SHCC has the responsibility to determine whether the IRB-approved Waiver of Authorization or the patient’s original Authorization, i.e., the stated purpose of the research or the authorized PHI, covers subsequent research analyses.\(^2\) If the SHCC determines that previous legal permissions do not cover the re-analysis request, then the researcher must obtain:

1. IRB approval for reanalysis using another Authorization;
2. Waiver of Authorization;
3. A Limited Data Set; or
4. A de-identified data set.

If a researcher has an IRB-certified exemption granted prior to the compliance date of April 14, 2003 and PHI is being used, disclosed, or accessed in the study, then the researcher must submit a new request for Exempt Certification.

**Implementation Policy 9-16:**

Research on PHI that is not de-identified which is being conducted under an IRB-certified exemption should be reviewed to determine if it meets the criteria for an IRB-approved Waiver of Authorization. It is the responsibility of the researcher to determine if a Waiver of Authorization is required and to apply for one.

**TRANSITION PROVISIONS**

**Implementation Policy 9-17**

The SHCC may use or disclose PHI for research purposes, either before or after the compliance date, if the SHCC obtained any one of the following legal permissions prior to the compliance date of April 14, 2003:

1. An authorization or other express legal permission from the individual to use or disclose PHI for research;

2. The informed consent of the individual to participate in the research; or

3. An IRB waiver of consent in accordance with the Common Rule.

**Implementation Policy 9-18**

During the transition period, the researcher must obtain a HIPAA-Authorization (see Appendix B) in the following circumstances:

1. If a waiver of informed consent was obtained prior to the compliance date of April 14, 2003, but informed consent is subsequently required; or

2. If the researcher wants to enroll new subjects after April 14, 2003, in an active study that requires the subject’s informed consent.

To facilitate research and to prevent the IRBs from undertaking the burden of renewing all protocols in which new subjects will be enrolled during the transition period, the UC IRBs have determined that the individual researcher may obtain the signed Authorization of new subjects concurrent with obtaining other required consent without IRB re-review of those research protocols. As such, for those studies that were in existence prior to April 2003, the SHCC can provide the PHI to the researcher pursuant to an Authorization signed by the new enrollee; the SHCC does not require an IRB Letter of Approval.

**Implementation Policy 9-19**

If a researcher collected data prior to April 14, 2003 for a specific research protocol and wants to use those data for a different research protocol after April 14, 2003, the researcher must comply with all HIPAA requirements outlined in Implementation Policy 9-1.

**RESEARCH DATABASES, INCLUDING TISSUE AND ORGAN BANKS AND ORGAN PROCUREMENT ORGANIZATIONS**

**Implementation Policy 9-20**

The SHCC may use or disclose PHI without Authorization for the creation of a research database, provided the researcher creating the database provides the SHCC with documentation that the IRB has determined that the specified Waiver of Authorization criteria were satisfied. The SHCC can use or disclose PHI maintained in the research database for future research studies as permitted by the Privacy Rule, i.e., pursuant to an individual’s Authorization or an IRB-approved Waiver. If the database was created prior to April 2003 without the individual’s legal permission or a Waiver of Consent from the IRB, the PHI contained in the database may only be used or disclosed for research purposes with either individual Authorization or IRB-approved Waiver.
Implementation Policy 9-21

An Organ Procurement Organization may only receive PHI without patient authorization for the purpose of facilitating organ, eye or tissue donation and transplantation. Research conducted on tissue obtained from a living donor requires an IRB approved protocol.

DISCLOSURES TO REGISTRIES

Implementation Policy 9-22

The SHCC may disclose PHI to registries, including those sponsored by academic or non-profit organizations, for research purposes, if such disclosures is:

a) Mandated by the state of California\(^{63}\) and made to the California Department of Health Services or its designated agent;

b) Mandated by federal law or policy\(^{64(2)}\) (such as the National Xenotransplantation Database) and made to the United States Department of Health and Human Services or its designee

c) Made pursuant to an IRB or Privacy Board approved waiver of authorization;

d) Made pursuant to the individual’s authorizations;

e) Consists of a de-identified data set; or

f) Consists of a limited data set made pursuant to a data use agreement to restrict further disclosure.

CLINICAL LABS THAT PARTICIPATE IN RESEARCH

Implementation Policy 9-23

UC clinical labs are, in the performance of certain functions, covered entities within the SHCC and, as such, must meet all of the HIPAA requirements for disclosing PHI to a researcher pursuant to an IRB-approved research protocol. When the analysis of data containing PHI is for the purpose of Quality Assurance, this function is a part of health care operations and is a permitted use and disclosure.

\(^{63}\) I.e., HEALTH AND SAFETY CODE SECTION 103875-103885, which authorizes the creation of cancer registries for epidemiological assessments of the incidence of cancer.

\(^{64}\) I.e., the National Exposure Registry maintained by US DHHS Agency for Toxic Substances and Disease Registry.
**PATIENT’S RIGHT TO ACCESS PHI CREATED IN A RESEARCH TRIAL**

**Implementation Policy 9-24**

PHI created as part of a research protocol and maintained in the SHCC’s designated record set\(^{65}\) is accessible to the research subject, with the exception that the SHCC may suspend the individual’s right to access\(^{66}\) the information created or obtained by the SHCC for a clinical trial while the clinical trial is in progress, provided the research participant agreed to this denial of access when consenting to participate in the trial. The researcher/health care provider must inform the individual that access will be reinstated at the conclusion of the trial.\(^{67}\)

**DISCLOSURES RELATED TO ADVERSE EVENTS**

**Implementation Policy 9-25**

A researcher may disclose PHI to the IRB, the SHCC, the federal Office of Human Research Protection, the FDA, research sponsors or other entity as required by regulations or by UC policy. The possibility of such disclosure should be included in the research Consent form. When the subject is participating in a protocol that requires a HIPAA Authorization and the SHCC must also provide information as required for monitoring of the study, the researcher may also seek Authorization from the subject for such disclosures. If Authorization is obtained, the SHCC will not have to provide an accounting of those disclosures if the subject/patient requests an accounting.

HIPAA-defined “operations activities” of the IRB, such as quality assurance, monitoring, auditing and reporting of adverse events, require the IRB to use PHI in its role as a member of the SHCC. Campuses may elect to establish a formal reporting relationship between the IRB and the SHCC so that adverse events arising from a research study that have implications for patient safety are appropriately reported.

**Implementation Policy 9-26: Redisclosure by Third Parties**

In order to assure research subjects that their PHI will remain confidential after disclosure to a research sponsor, the University should endeavor to gain assurance from the research sponsor that PHI will not be used or disclosed for purposes other than those for which it was collected or created. Even if research sponsors agree to use or disclose PHI only for purposes for which it was collected or created, the Privacy Rule requires that the research Authorization notify the subject of the potential for information disclosed pursuant to the Authorization to be subject to redisclosure by the recipient and to no longer be protected by the HIPAA Privacy Rule.\(^{68}\) The Authorization

\(^{65}\) Designated record set includes medical records and billing records about individuals and maintained by or for a covered health care provider. See definition in Standard Three.

\(^{66}\) See Standard: Patient’s Right to Access or Copy the Designated Record Set

\(^{67}\) OCR Privacy Rule Guidance, December 2002, p. 93.

\(^{68}\) 45 CFR 164.508(c)(2)(iii)
may include language concerning other protections afforded individually-identifiable health information, such as those found in state law.

The HIPAA Taskforce and the UC Office of the General Counsel is currently reviewing state law regarding recent amendments of the California Medical Information Act to determine if the amended language provides greater protection for the confidentiality of individually identifiable health information when that information is used by pharmaceutical companies.

**Standard Ten: Use and Disclosure of PHI for Institutional Advancement and External Relations**

- Fundraising
- Media relations and external communications
- Marketing
- C.F.R. 164.508 and 164.514

The Privacy Rule applies to all SHCC workforce members, including volunteers, and entities that carry out institutional advancement, development or external relation functions and activities on behalf of or for the SHCC’s individual or institutional health care providers. When the SHCC contracts with business associates/consultants or works with institutionally-related foundations that are separate legal or third party entities to carry out development or external relations activities on the SHCC’s behalf, those entities are subject to a business associate agreement (or confidentiality agreement, in the case of foundations who may be subject to tax code provisions that do not allow those institutions to enter into a business association agreement) and must comply with the Privacy Rule.

**FUNDRAISING BY THE SHCC**

The SHCC can use—or disclose to business associates or institutionally related foundations—the following information about the individual for the purpose of raising funds for the SHCC’s benefit:

1. An individual’s demographic information⁶⁹; and
2. Healthcare dates of service.

**FUNDRAISING ACTIVITIES THAT REQUIRE THE PATIENT’S AUTHORIZATION**

Uses and disclosures of all other PHI, including the individual’s diagnosis or treatment protocol, require the individual’s authorization. After April 2003, the SHCC cannot use disease-specific data bases for fundraising activities unless the patient has authorized that use. The Privacy Rule

---

⁶⁹ Demographic information is the individual’s name, date of birth, gender, ethnicity, insurance status, address and other contact information— but does not include information about the individual’s illness or treatment (Privacy Rule December 2000 Preamble)
preamble suggests that covered entities utilize the time prior to April 2003 to develop lists under Authorizations that allow for disease or treatment specific fundraising activities.  

**MARKETING BY THE SHCC**

The Privacy Rule distinguishes marketing activities from those health care communications about goods and services that are essential for quality health care. Marketing is:

1. A communication that encourages a recipient of the communication to purchase or use the product or service; or

2. Arrangements where the SHCC discloses PHI to another entity (e.g., gives lists of patients’ demographics and dates of service to a third party);

3. Arrangements where the SHCC provides PHI to another entity in exchange for direct or indirect remuneration (e.g., sells patients’ PHI) in order for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

**MARKETING ACTIVITIES THAT REQUIRE THE PATIENT’S AUTHORIZATION**

The SHCC must obtain a written Authorization for all marketing communications, and the Authorization must state whether the marketing involves direct or indirect remuneration to the SHCC from a third party. Examples of marketing activities that require the patient’s Authorization include:

1. A health plan sells a list of its members to a company that sells blood glucose monitors so that the company can market its product to the members;

2. A drug manufacturer receives a list of patients from the SHCC in exchange for some form of remuneration and uses that list to send medication discount coupons to the patient;

3. The SHCC provides names of pregnant women to baby formula manufacturers or magazines in exchange for some type of remuneration (e.g., an advertisement for the medical center in the magazine); or

4. The SHCC provides a list of patient names to a telemarketer or other third party business associate for a health care communication that is not considered marketing, but then allows the business associate to use the list to market its own products.  

---

70 *IBID, 53223, “Covered entities are provided a period in which to come into compliance with the Privacy Rule. One purpose of the compliance period is to allow sufficient time to undertake actions such as obtaining the legal permission that would permit databases to continue to operate after the compliance date.”*

71 If the telemarketer or other third party is a business associate of the SHCC, it must agree by contract to use the PHO only for communicating on behalf of the SHCC and not to market its own goods or services.
TWO EXCEPTIONS TO THE REQUIRED PATIENT’S AUTHORIZATION FOR MARKETING

The SHCC may engage in the following communications without authorization:

1. The communication occurs in a face-to-face encounter between the SHCC or covered entity and the individual (A face-to-face encounter is not: telephone, mail, fax or the internet); or

2. The communication involves a promotional gift of nominal value.
   a) Free package of formula and other baby products; or
   b) Free pharmaceutical samples, regardless of their value.

SHCC HEALTH CARE COMMUNICATIONS THAT ARE NOT MARKETING AND DO NOT REQUIRE THE INDIVIDUAL’S AUTHORIZATION

A communication is not defined as marketing if the health care communication enhances the individual’s access to quality care; promotes health in a general manner; or does not promote a specific product or service from a particular provider. The Privacy Rule allows the following types of health care communications and does not define them as marketing activities:

1. A communication to describe a health-related product or service that is provided by a covered provider or included in a plan of benefits of the health plan, including communications about:
   a) A medical center’s new specialty group or the acquisition of new equipment that goes out through a general mailing;
   b) A physician who has developed an anti-snore device could send a flyer to all her patients; an ophthalmologist could send her patients discount coupons for eye-exams or eye-glasses;
   c) The participating providers and health plans in a network or the benefits covered by a health plan, including a mailing to subscribers who are approaching Medicare age about a Medicare supplemental plan;
   d) Changes in the health plan; or
   e) Health related products or services available only to a health plan enrollee that add value to, but are not part of, the plan of benefits.

2. Communications that provide information about the individual’s treatment, including a:
   a) Referral to a specialist for follow-up tests,
   b) Prescription refill reminder, even if a third party pays for the communication.72

72 The simple receipt of remuneration does not transform a treatment communication into a commercial product or service. OCR Privacy Rule December 2002 Guidance, p. 73.
3. Communications regarding case management or care coordination for the individual, to direct or recommend alternative treatments, therapies, health care providers, or settings of care, and communications that promote health in general, including

   a) An endocrinologist shares PHI with several behavior management programs to determine which program best suits the needs of the patient;

   b) A hospital social worker shares PHI with nursing homes in the course of recommending the next level of care;

    c) Health education or wellness classes, support groups, health fairs;

    d) Mailings reminding women to get an annual mammogram;

    e) Mailings providing information about how to lower cholesterol, use of various ointments or medication that could be alternative medicine, or other disease prevention activities;

    f) Communications about government and government-sponsored programs—e.g., Medicare supplemental payments and SCHIP;

    g) Newsletters, so long as the content does not meet the definition of marketing; and

    h) Population-based activities to improve health or reduce health care costs as set forth in the definition of “health care operations.”

COMMUNICATIONS WITH THE MEDIA

Calls from the Media or Others Regarding an Individual’s Status

When the media contacts the SHCC to request specific information about an individual who may be a patient of the SHCC, the media must first identify the individual by name. If the individual has been provided with the Notice of Privacy Practices and has not limited the information provided in the facility directory, the SHCC may confirm that the individual is in the institution, the individual’s location and general condition (stable, serious, critical).

If the individual (e.g., a VIP) has not been given an opportunity to limit or restrict the information in the facility directory because the care is being provided in an emergency situation, the SHCC must make a professional judgment as to whether the individual would otherwise permit the SHCC to provide the information included in the facility directory.

Other Media Relations Activities

73 A medical center’s Wellness Department could start a weigh-loss program and send a flyer to all patients seen in the medical center over the past year who met the definition of obese, even if those individuals are not specifically seen for obesity. OCR December 2002 Privacy Rule Guidance, p. 71.
The Privacy Rule does not define “media and community relations” or provide specific guidance regarding these activities. By contrast, the Privacy Rule defines both marketing and fundraising and provides specific implementation requirements.

Therefore, the UC SHCC has determined that public affairs, community and media relations are activities that meet the definition of health care operations as “business management and general administrative activities of the entity.” These activities include:

1. Providing crisis communications expertise and serving as members of the crisis response team;
2. Determining the newsworthiness of stories and other communications that support management and the SHCC’s operations; or
3. Participating on the patient care team in order to protect the patient’s privacy, including that of VIPs, celebrities and others.

The SHCC’s academic health centers often receive requests from the media for specific public or community relations information or patient stories. Also, the SHCC, in order to carry out its administrative operations and its mission of service to and education for the community, often requires some health information regarding an individual or an individual’s stay in the medical center in order to provide communications and stories to the public regarding the services of an academic medical center. In order to identify individuals for these communications, the SHCC’s Office of Development or External Relations can:

1. Educate the SHCC’s direct treatment providers that when these situations occur, the patient’s provider or provider team should make the initial contact with the patient and obtain the individual’s permission to be contacted by the Office of Development or External Relations. If the Office of Development or External Relations contacts the patient, they must then obtain a signed Authorization for use or disclosure of PHI; or
2. The SHCC can seek Authorization upon admission or discharge for contact by the Office of Development for patient stories or photos. This Authorization can be combined with other Authorizations and given to the patient as a Compound Authorization.

**STANDARD TEN: IMPLEMENTATION POLICIES**

**Implementation Policy 10-1: Fundraising**

Development and Institutional Advancement Offices within the SHCC may use or disclose the individual’s demographic information and health care date of service for fundraising activities, so long as:

1. The SHCC defines demographic information only as the individual’s name, date of birth, gender, ethnicity, insurance status and address and other contact information, but does not include information about the illness or treatment;

---

74 Definition of health care operations, p. 6, HIPAA Privacy Regulation Text, October 2003.
2. The SHCC’s Notice of Privacy Practices states that the SHCC may contact the individual to raise funds for the SHCC and may use, or disclose certain information (demographic and dates of health care service) to a business associate or institutionally related foundation, for the SHCC’s own fundraising purposes;

3. When the SHCC provides fundraising materials to the individual, the SHCC provides the individual with a clear and simple way to opt out of any future fundraising communications;

4. The SHCC’s individual or institutional providers and development departments implement a reasonable and workable process for recording and tracking all individual “opt outs”;

5. To provide for good faith efforts to safeguard individual PHI, the direct treatment provider should make the initial contact, either in writing or face-to-face, for those development activities that an individual could interpret as directly linked to her or his diagnosis or treatment and must obtain the individual’s Authorization for contact by others within the SHCC; and

6. In all cases, it should be made very clear that the individual can request that there be no further fundraising communications from the individual provider or SHCC.

**Implementation Policy 10-2: Fundraising**

In order to create lists for fundraising purposes by Development and Institutional Advancement Offices (IA) within the SHCC:

1. University faculty physicians can provide IA with a list that includes their patient’s demographics or the IA Office can ask faculty physicians to provide a list of individuals (patients and others) and their demographics to create a list for use for fundraising purposes so long as:

   a) Disease diagnosis is not used as the criterion for developing the list—e.g., the faculty member or IA Office cannot go to the data manager and ask that he or she provide a list of all of the faculty member’s patients who match to a certain disease diagnosis or treatment protocol;

   b) All fundraising material\(^\text{75}\) provides the recipient with a way to opt out from receiving any additional information;

   c) Lists provided by faculty physicians may also include individuals not directly under the care of the SHCC;

   d) Written solicitations should be worded in such a way as to not suggest that the sender of the solicitation letter knows the individual’s disease diagnosis or

---

\(^{75}\) Fundraising materials include all fundraising solicitations: major gift proposal, newsletters that solicit donations, event invitations, etc.
treatment unless the recipient has specifically Authorized the use of that PHI for fundraising purposes (for example, VIP donors who want their names linked to a specific appeal); and

e) Faculty and others should coordinate all fundraising efforts with IA;

2. The individual’s health care provider or provider team must obtain the individual’s written Authorization to provide disease or treatment specific information to IA. The SHCC must maintain the Authorization for six years;

3. The SHCC can seek authorization from the individual at admittance or discharge that would allow direct contact by IA to discuss fundraising or gift opportunities that are disease specific or related to the individual’s healthcare treatment. The Authorization may be combined with other Authorizations under a Compound Authorization; and

4. The SHCC cannot receive PHI (individually identifiable information that includes the individual’s disease or treatment information) from members of its workforce, including volunteers, for purposes of fundraising activities unless the individual authorizes the use of the PHI for fundraising activities by the SHCC.

Implementation Policy 10-3: Fundraising

The SHCC faculty member or provider can directly contact his or her patient for fundraising, development or external relations and media purposes using the individual’s demographics and/or dates of service. However, the provider must obtain the patient’s Authorization in order to provide to or request PHI from staff, data managers, the Office of Institutional Advancement or SHCC workforce members in order to use disease or treatment specific information for fundraising or other appeals.

Implementation Policy 10-4: Fundraising

The SHCC does not have to provide an accounting for disclosures that use only the patient’s demographics and dates of service for fundraising activities because the Privacy Rule defines those activities as operations. Patient Authorized disclosures do not require an accounting.

Implementation Policy 10-5: Fundraising

The SHCC may use the Facility Directory\textsuperscript{76} to identify individuals who may be receiving care in the covered entity and to personally contact them during their stay as a part of the development activities of the SHCC.

\textsuperscript{76} The SHCC may use a patient’s demographics for fundraising purposes without Authorization. The Facility Directory contains only the patient’s name and location, a subset of the full set of demographic information.
Implementation Policy 10-6: Marketing

The SHCC must obtain a written Authorization for all marketing communications, and the Authorization must state whether the marketing involves direct or indirect remuneration to the SHCC from a third party. (See narrative discussion of marketing)

Implementation Policy 10-7: Marketing/No Authorization Required

The SHCC may engage in the following marketing activities without authorization:

1. The communication occurs in a face-to-face encounter between the SHCC or covered entity and the individual (A face-to-face encounter is not: telephone, mail, fax or the internet); or
2. The communication involves a promotional gift of nominal value.
   a) Free package of formula and other baby products; or
   b) Free pharmaceutical samples, regardless of their value.

Implementation Policy 10-8: Health Care Communications

A communication is not defined as marketing if the health care communication enhances the individual’s access to quality care; promotes health in a general manner; or does not promote a specific product or service from a particular provider. (See narrative for specific examples of health care communications that are not marketing and do not require an Authorization.)

Implementation Policy 10-9: Health Care Communications

An individual may request or negotiate limits on the uses and disclosures of PHI for those healthcare communications that are not marketing. If the individual requests those restrictions, the SHCC does not have to agree, but should document its denial and the reason for denial.

Implementation Policy 10-10: Health Care Communications

Although individuals may request confidential forms of communication of PHI to prevent such practices, the SHCC should make it routine practice not to send health care communications that may include a patient’s PHI, test results, or appointment reminders (when those reminders include specific diagnoses) on a post card or by fax to an unsecure location.

Implementation Policy 10-11: Health Care Communications

The SHCC and covered individual providers must be mindful that communications to an individual to recommend, purchase or use a product or serve as part of treatment, case management or care coordination could be considered a violation of other statutes or regulations administered by the Department of Health and Human Services, the Department of Justice or other federal agencies if the provider uses his or her relationship with individuals to systematically

77 A fax number where the identity of the recipient is not clear or a number that has not been specifically provided by the individual for personal communications.
market the goods and products of third parties (e.g., home health nurses recommending durable medical equipment companies). Nothing in Privacy Rule can be construed as amending, modifying or changing any rule or requirement related to any other Federal or State statutes or regulations, the anti-kickback statute, safe harbor regulations, Stark law and HIPAA statute on self-referral. 78

Implementation Policy 10-12: Media or External Relations

In determining the newsworthiness of a story regarding the SHCC’s mission, the media and/or external relation staff may request PHI from physicians and other members of the provider team and use that information in making the determination. However, in all circumstances, the External or Community Relations Office must limit requests to physicians or others to the minimum necessary to achieve the purpose of the activity. Information used internally to determine the newsworthiness of a story should be restricted to: age, gender, ethnicity, dates of admission or discharge, city of residence, occupation and general disease or diagnosis.

Implementation Policy 10-13: Media or External Relations

In order to provide PHI to an outside media organization, the SHCC must obtain the patient or member’s Authorization using an Authorization that contains all the Privacy Rule required elements and retain the signed Authorization for six years. The HIPAA Taskforce has prepared an Authorization Form that meets all the required Privacy Rule elements and which should be used for these purposes.

Implementation Policy 10-14: Media or External Relations

When the media or other members of the public (including a family member) contact the SHCC to request specific information about an individual, the caller must first identify the individual by name. If the individual has been provided with the Notice of Privacy Practices and has not limited the information provided in the facility directory (inpatient activities), the SHCC may confirm that the individual is in the institution, the individual’s location and general condition (stable, serious, critical).

If the individual (e.g., a VIP) has not been given an opportunity to limit or restrict the information in the facility directory because the care is being provided in an emergency situation, the SHCC must make a professional judgment as to whether the individual would otherwise permit the SHCC to disclose any information to an outside caller.

The same principle should apply in the outpatient setting, except that in the outpatient or clinic setting (e.g. Student Health Services), the person receiving the call may be able to ask the patient if s/he will accept the call.

Implementation Policy 10-15: Databases

The Privacy Rule does not grandfather the release of PHI in existing databases, unless the SHCC obtained the required legal permissions that would permit databases to continue to operate after

78 OCR Privacy Rule December 2002 Guidance, p. 75.
April 2003. For institutional advancement, fundraising and external relations purposes, current databases containing patient disease or diagnosis specific information must be updated with the individual’s Authorization to include their PHI in the database or that information cannot be used for future communications. For the purpose of developing an IA database for future media or external relations communications, a signed Authorization must be obtained from the patient. The release of PHI from existing or future databases to the media or through a publication will require a separate Authorization that meets the regulatory requirements.

**Standard Eleven: A Patient’s Right to Request Restriction on Uses and Disclosures CFR 164.522**

- Acceptable Restrictions
- Individuals Involved In The Patient’s Care

The Privacy Rule provides the individual with certain rights regarding his or her PHI and requires the SHCC to respond when the individual chooses to exercise those rights. Unlike many other standards within the Privacy Rule where the SHCC is allowed some flexibility in developing workable policies and procedures to comply, the Privacy Rule is quite prescriptive, in most cases, as to when, how and what the SHCC must do when responding to an individual’s request.

**STANDARD ELEVEN IMPLEMENTATION POLICIES**

**Implementation Policy 11-1**

The SHCC must provide the individual with an opportunity to request restrictions of uses and disclosures of PHI for treatment, payment and operations. While most restriction requests could occur at admission, the individual may request restrictions at any time.

The SHCC does not have to agree to a request for restrictions for purposes of treatment, payment and operations, but if the SHCC agrees to restrictions, it must respect and abide by those restrictions, except when the individual needs emergency treatment.

Although not considered a “restriction” under the Privacy Rule, a patient may elect to “opt out” of the Facility Directory of an inpatient facility. This opt out will restrict access to the patient’s location or condition if an individual (media, clergy, family member, stranger, etc.) identifies the individual by name and asks regarding the patient’s condition. Facility Directory opt out requests must be honored by the SHCC.

**Implementation Policy 11-2**

The SHCC may terminate its agreement to the restriction if the individual agrees to or requests a termination in writing or an oral requested is documented. The SHCC may also inform the individual that it terminates its agreement for a restriction.

**Implementation Policy 11-3**

The SHCC should provide and document as follows:
1. All Restriction Requests must be in writing;
2. Provide a written response to the restriction request;
3. Document any agreed to restrictions; and
4. Document any oral requests from the patient to terminate the restriction;

Implementation Policy 11-4

In general, covered entities within the SHCC will not accept requests for restrictions because of the difficulty of providing treatment, carrying out necessary operations (including teaching) and obtaining payment for services rendered if the SHCC cannot use or disclose PHI for those purposes. However, the SHCC will consider requests for restrictions due to social stigma, VIP status, or those situations where certain disclosures could cause harm to the individual (for example, victims of domestic abuse). In most cases, the SHCC can accommodate these by providing the individual with the opportunity to opt out of the Facility Directory or use an alias.

Implementation Policy 11-5

The patient has the right to request restrictions on PHI used or disclosed to family members, friends, or relatives involved in the individual’s care. In certain circumstances the SHCC will have to provide those restrictions as requested. In order to disclose PHI to family members or friends of the individual or any other person:

1. The individual must identify the individual as involved in his/her care;
2. The PHI must be directly related to the individual’s involvement in care;
3. The PHI is for purposes of notifying individuals responsible for the person’s care regarding his/her general condition or death;
4. If the patient is not present, the SHCC must use its best judgment in determining whether the limited disclosure of PHI is in the best interest of the individual; and
5. If the family member or friend is present with the individual, the SHCC can only use or disclose PHI to the family member or friend only:
   a) If the patient has had an opportunity to object to the use or disclosure and does not; or
   b) Agrees to the use or disclosure; or
   c) In the professional judgment of the provider team, the patient would not object.

Implementation Policy 11-6

State law is more restrictive and protective for mental health patients regarding access by family members and friends to PHI. When a health care provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental
health records requested by the patient, the provider may decline to permit inspection or provide copies of the records to the patient, subject to the following conditions:

**Implementation Policy 11-7**

UC workforce members may want to request restrictions in order to prevent unwarranted access to medical records by colleagues and the employer. In these cases, the Privacy Rule prohibits access to an employee’s PHI except when it is necessary for a member of the workforce to perform his or her job, including the provision of care to the employee, who is also a patient. Federal and state law currently prohibit an employer’s access to medical records except under those circumstances either required by law (e.g., workplace injury or illness, medical surveillance of the workforce when the Notice describes this practice) or when Authorized to by the employee. If SHCC workforce members comply with the Privacy Rule and System Standards there should be no unwarranted access to a workforce member’s PHI or medical record set by a fellow workforce member.

If there is unwarranted access, it is a violation of The Privacy Rule and University policy.

---

**Standard Twelve: A Patient’s Right To Request Confidential Communications. CFR 164.522**

**STANDARD TWELVE IMPLEMENTATION POLICIES**

**Implementation Policy 12-1**

The SHCC must permit individuals to request and must accommodate reasonable requests to receive communications of PHI from the SHCC by alternative means of communication or to alternative locations. The SHCC cannot require the individual to explain the reason for the request.

**Implementation Policy 12-2**

The SHCC will accommodate requests if:

1. Requests are in writing to the responsible SHCC individual with specific instructions as to location, address or fax number and include individual’s signature and dated;

2. The request is for electronic communications via email or fax, so long as the individual has provided a signed request for electronic communications; and

3. When the requests are for mailed communications, other than standard first class mail, the individual provides payment in advance for all costs of mailing to one or more alternative locations (e.g., Fedex, express mail, etc.).

**Implementation Policy 12-3**

The responsible individual who has received the request should maintain a record of all requests, provide a written response to the request and maintain a copy of the response.
Implementation Policy 12-4

Although individuals can request confidential forms of communication of PHI to prevent such practices, the SHCC should make it routine practice not to send a patient’s PHI, test results, or appointment reminders (when those reminders include specific diagnoses) on a post card or by fax to an unsecure location.

Standard Thirteen: A Patient’s Right to Access and Copy the Designated Record Set

- CFR 164.524

STANDARD THIRTEEN IMPLEMENTATION POLICIES

Implementation Policy 13-1

The SHCC must provide the individual with an opportunity to access, inspect, and obtain a copy of the individual’s Designated Record Set.

Implementation Policy 13-2

Covered entities within the SHCC must document the designated record sets that are subject to access by the individual and the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Implementation Policy 13-3

The Notice of Privacy Practices must provide information as to how the individual can request access. Requests to access, inspect or copy the DRS must be in writing to an individual or office specified for these purposes. The specified individual and office will be responsible as follows:

1. To grant access or provide a written denial of access within 30 days;
2. To grant access or provide written denial of access within 60 days if the designated record set is located or maintained off-site and not readily accessible;
3. To advise the individual in writing if the SHCC does not maintain the DRS;
4. To provide the individual with a written reason for a one-time delay of no more than 30 days and a specific date when the SHCC will take action on the request; or
5. To provide providing a written denial of the request as allowed under IP 13-7.

Implementation Policy 13-2

If it is reasonable to do so, the SHCC must provide the information in the format requested by the individual, in a readable hard copy or in some other form that can be agreed upon by the SHCC and the individual. The SHCC cannot deny access or refuse to provide copies of the information based on a disagreement as to format.
Implementation Policy 13-3

If the information requested is located in more than one designated record set or at more than one covered entity within the SHCC, the individual is responsible for identifying the site(s) and requesting in writing from each of the different entities. For example, if an individual requests access to a designated record set maintained by two separate UC medical centers or the business associate of one medical center, the individual must contact each of the covered entities or medical centers since the SHCC does not have a central record-keeping system.

Implementation Policy 13-4

In order to expedite the response to the written request for access, the SHCC should:

1. Provide the individual with a Request for Access Form that allows the individual to specify the scope, format, and the option of purchasing a summary of the PHI requested;

2. Provide the individual with a list of the fees for summarizing the information, if the individual requests a summary of the DRS;

3. Provide the individual with convenient times and location for inspecting or obtaining a copy of the information; and

4. Request the location for mailing the information.

When an individual contacts the specified office or individual to request access, the SHCC can provide the Request for Access Form in order for the individual to comply with the SHCC’s requirement that all requests be in writing.

Implementation Policy 13-5

The SHCC will charge a reasonable, cost-based fee for copying (including supplies and labor), postage, and the cost of creating a summary if requested. If the request comes from parties other than the individual or the personal representative, the fee limitations do not apply to those individuals or entities (e.g., attorneys).

Implementation Policy 13-6

The SHCC is not required to provide access to the following information:

1. Psychotherapy notes;

2. Information compiled in anticipation of a civil, criminal or administrative action or proceeding;

3. Information not available because of restrictions under the Clinical Laboratory Improvements Amendments of 1988 (CLIA);

4. Oral communications;
5. The request is to a correctional institution or to the SHCC under the direction of a correctional institution, if release of the information would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmate or an officer or employee of the correctional institution;

6. The PHI has been created or obtained by a covered health care provider in the course of research that includes treatment and in the research consent process, the individual has agreed he or she will not be allowed access to that PHI so long as the research is in progress;

7. Information that is restricted by the Privacy Act; or

8. Information was obtained from a third party under a promise of confidentiality.

Implementation Policy 13-7

If the individual is allowed a review of the denial, the SHCC may deny access to the DRS in the following circumstances, so long as California law does not preempt the Privacy Rule in this circumstance79:

1. If a licensed health care professional has determined that access could endanger the life of the individual or another person;

2. If the requested information references another person (except a health care provider) and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to the other person; or

3. If the request is made by the individual’s personal representative, and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to the individual or another person.

The SHCC may only deny access to that portion of the DRS described in a through c, above. To the extent possible, the individual must have access to all other information.

Implementation Policy 13-8

If the SHCC denies access, the SHCC must provide a written denial to the individual that:

1. Is in plain language;

2. Contains the basis for denial;

3. Provides for review rights;

4. Describes how the individual may complain to the SHCC; and

79 In some cases, California law requires greater access for behavioral or mental health patients. Individuals responsible for providing access should consult with Counsel.
5. Includes the name or title, telephone number of the University or system Privacy Officer designated to receive complaints.

**Implementation Policy 13-9**

When access is denied and the individual requests a review of the denial (for IP 13-7 circumstances only), the SHCC will designate a licensed health care professional, who did not participate in the denial of access decision, to act as a reviewing official. Within a reasonable time period, the reviewing official must provide the individual with a written decision based on the standards in Implementation Guideline 13-7.

**Standard Fourteen: The Patient’s Right to an Amendment of the Designated Record Set.**

**Implementation Policy 14-1**

An individual has a right to request that the SHCC amend the medical record or other information in the DRS. Under California law, the patient also has a right to append information to the medical record. The individual must provide a written request to the SHCC for the amendment and provide the reason to support the requested amendment. The SHCC should maintain the written request for 6 years.

**Implementation Policy 14-2**

The SHCC must act on the individual’s request for an amendment no later than 60 days after receipt of such a request by either accepting and making the amendment or denying the request in writing. If the SHCC is unable to act on the amendment within 60 days, it may have a one-time delay of no more than 30 days by providing (within the initial 60 days) the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed.

**Implementation Policy 14-3**

If SHCC accepts the amendment in whole or in part, the SHCC must:

1. Identify the affected records and link the amendment to the affected records in the designated record set;
2. Inform the individual in a timely manner that the amendment has been made;
3. Obtain the individual’s identification of and agreement to have the SHCC notify those persons with whom the amendment needs to be shared; and
4. Make a reasonable effort to notify those persons who the SHCC knows has the designated record set that has been amended. These persons include those identified by the individual and others, including business associates, who should amend the DRS because reliance on the unamended DRS could cause harm to the individual.
**Implementation Policy 14-4**

The SHCC may deny an individual’s request for amendment, if it determines that the record:

1. Is accurate and complete without amendment;
2. Is not part of the designated record set;
3. Would not be available for inspection by the individual; or
4. Was not created by the SHCC, unless the individual provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment.

**Implementation Policy 14-5**

If the SHCC denies the request for amendment, the SHCC must provide in writing:

1. A written denial (in plain language) within the time limits described in Implementation Policy 14-2;
2. A basis for the denial (Implementation Policy 14-4);
3. The process by which the individual may submit a written statement disagreeing with the denial, including the basis for disagreement and the SHCC’s accepted length of the statement of disagreement, which should be the same length as required under California law;
4. A statement that if the individual does not submit a written statement of disagreement, the individual may request that the SHCC provide the individual’s request for amendment and the written denial with any future disclosure of the PHI subject to the requested amendment; and
5. The process by which the individual may make a complaint to the SHCC, including the title, name, contact number of the University Privacy Office or Officer.

**Implementation Policy 14-6**

The SHCC may also prepare a rebuttal of statement of disagreement, but must provide the individual with a written copy of the rebuttal statement.

**Implementation Policy 14-7**

Even if the SHCC denies the request for an amendment, the SHCC must link or append all relevant, written documents pertaining to the request to the information that is subject to the request, including the written request, denial, statement of disagreement and rebuttal.
Implementation Policy 14-8
If the SHCC denies the request for an amendment and the individual has either submitted a statement of disagreement or a request as defined in Implementation Policy 14-5, the SHCC must include all material described in Implementation Policy 14-7 or the SHCC’s summary of that information, in any future disclosures of the PHI or information that was the subject of the individual’s request.

Implementation Policy 14-9
When a subsequent disclosure of the information that was the subject of the request is by a standard transaction (see definitions) that prevents amending the information in the form of the transaction, the amendment or other information (Implementation Policy 14-8) may be separately transmitted.

Implementation Policy 14-10
If the SHCC denies the individual’s request to amend, California law requires that the request be attached or appended to the unamended record set. The SHCC cannot refuse a patient’s request to append information.

Implementation Policy 14-11
If the SHCC is informed by another covered entity of an amendment to an individual’s PHI, the SHCC must amend the PHI in its DRS.

Standard Fifteen: Individual’s Right to Request an Accounting of Disclosures of PHI.
The individual has a right to receive an accounting of disclosures of PHI that have been made by the SHCC within the last six years, or from April 2003 forward, whichever occurred last. The individual may request an accounting for any time period less than the six years.

Many of the disclosures that require an accounting are listed in the Privacy Rule under 164.510, “Uses or disclosures for which an authorization or opportunity to agree or object is not required.” If the individual has not had an opportunity to agree, object or Authorize the disclosure, the principle of the Privacy Rule is that the individual has the right to know about the disclosures by requesting an accounting. In some cases, California state law may be more protective and require notice to or consent by the individual who is the subject of the disclosures under 164.510. Consult with Counsel when questions arise regarding state versus federal law.

CFR 164.510, 164.528

Implementation Policy 15 –1: Required Accounting
The SHCC must have in place policies and procedures to provide accounting for disclosures to or for:
1. A business associate (except for treatment, payment or operations);

2. Those entities or individuals as required by law (except where excepted in Implementation Policy 15-2);

3. Public health activities (except for Disaster Relief purposes);

4. The individual’s employer when the SHCC provides health care to the employee at the request of the employer or when the disclosure is to the employer for medical surveillance in the workforce or a work-related illness or injury and for worker’s compensation if not authorized by the individual (the Notice of Privacy Practices must provide Notice that the provider can disclose to the employer as required by law for these purposes);

5. A government authority authorized to receive reports about suspected abuse, neglect or domestic violence (the SHCC should have notified the individual of the disclosure unless it believed it was not in the individual’s best interest);

6. Health oversight activities for health oversight activities;

7. Judicial and administrative proceedings (unless disclosure has been suspended by the agency);

8. To law enforcement officials for law enforcement purposes, including information regarding a suspect, fugitive, material witness or missing person or victims of crime or crimes on premises (unless disclosure has been suspended by the agency);

9. Transplant purposes to organ procurement organizations;

10. Avert a serious threat to the health or safety (except when an suspension of accounting is requested as described below);

11. Specialized government functions (except for national security and intelligence activities and law enforcement custodial activities as described below), including for protected services for the President and others;

12. Military and veterans activities;

13. Administration of public benefits programs;

14. Research disclosures under a Waiver of Authorization (see special accounting procedures under Accounting Standard), including what HIPAA defines as “review preparatory to research” but UC IRB policies defines as research; and

15. Disclosures by whistleblowers or workforce member crime victims;

**Implementation Policy 15-2: Exception to the Accounting Requirement**

The Privacy Rule requires the SHCC to provide a patient with an accounting of the disclosures of the patient’s PHI made by the SHCC in the six years prior to the date on which the accounting is requested **EXCEPT** for the following uses and disclosures to or for:
1. The individual;

2. Treatment, payment and health care operations;

3. Business Associates who have entered into either a Business Associate Agreement or Amendment as required, so long as the disclosure is for payment and operations or when the individual has signed an Authorization for the disclosure;

4. Incidental to treatment, payment and operations;

5. Authorized by the individual with a signed HIPAA-authorization;

6. Part of a Limited or Deidentified Data Set;

7. Facility directory (individual must have an opportunity to agree or object);

8. Individuals involved in the patient’s care (individual must have an opportunity to agree or object), including others when the individual is present and to persons who should be notified of the individual’s location, general condition or death;

9. Disaster relief purposes;

10. National security or intelligence purposes to authorized federal officials for the conduct of lawful intelligence, counter-intelligence and other national security activities authorized by the National Security Act;

11. Correctional institutions or law enforcement officials for custodial situations so long as the use or disclosure is for: the provision of health care, health and safety of the individual or other inmates or persons responsible for transporting inmates; law enforcement on the premises and for maintaining the good order of the correctional institution;

12. Health oversight or law enforcement agency who request temporary suspension of accounting because it may impede their activities (see documentation requirement); and


**Implementation Policy 15-3**

The individual must provide the SHCC with a written request for an accounting, and the SHCC should maintain the written request for six years.

**Implementation Policy 15-4**

The SHCC must respond to the written request for accounting within 60 days of receipt of the request. If the SHCC is unable to provide the accounting within 60 days, the SHCC may have a one-time delay of 30 days by providing the individual with a written statement of the reasons for the delay and the date when the SHCC will provide the accounting.
**Implementation Policy 15-5**

The SHCC must provide the individual with a written accounting that meets the following requirements:

1. The date of the disclosure;
2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed;
4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of a written request for disclosure under 164.502 (a)(2)(II) or 164.512 or a copy of the individual’s written authorization; and
5. If there have been multiple disclosures of the individual’s PHI to the same person or entity for a single purpose, the accounting may include the information required for the first disclosure, date of the last disclosure and the number of disclosures made during the accounting period.

**Implementation Policy 15-6**

If the disclosure of the individual’s PHI is pursuant to an IRB Waiver of Authorization and includes disclosures for a research purpose that involves 50 or more individuals, the SHCC may provide the individual with the following information to satisfy the accounting request:

1. Name of the protocol or other research activity;
2. A description in plain language of the research activity, including the purpose of the research and criteria for selecting the records;
3. A brief description of the type of PHI disclosed;
4. Date or time period during which such disclosure may have occurred;
5. The name, address and telephone number of the entity that sponsored the research and the researcher to whom the PHI was disclosed;
6. A statement that the PHI may or may not have been disclosed for a particular research activity; and
7. If the research entity has provided an accounting as described in a – f, the SHCC shall, at the request of the individual, assist in contacting the entity that sponsored the research and researcher.

**Implementation Policy 15-7**

The SHCC must provide the first accounting to an individual within a 12-month at no charge. The SHCC may charge a fee for subsequent requests from the same individual if the SHCC advises the
individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request in order to reduce or avoid a fee.

**Implementation Policy 15-8**

The SHCC must document and retain the documentation for 6 years:

1. The information required to be in the accounting;

2. The written accounting that is provided to an individual; and

3. The titles of the persons or officer responsible for processing accounting requests.

On an annual basis, each of the covered entities within the SHCC will provide to the system Privacy Officer a list of the accountings provided to individuals during the annual reporting period. The list of accountings need only include the following:

Patient #1 provided with an accounting for ___________(time period). The written accounting complied with the requirements of University Policy and the Privacy Rule.

---

**Standard Sixteen: Permitted Uses and Disclosures to Business Associates (BA).**

- 45 CFR 164.502(e), 164.504(e), 164.532 (d)(e)

The SHCC’s entities or workforce members must enter into Business Associate (BA) relationships and contracts with BA, defined as those outside vendors or contractors who create, receive, use or disclose PHI for or on behalf of SHCC entities or workforce members. In other words, the SHCC engages the BA to carry out a number of functions on its behalf, one of which is a function that specifically requires the creation, use or disclosure of PHI. By contrast, the SHCC may engage non-BAs to carryout activities on its behalf that may or may not involve PHI, and any use or disclosure of PHI in those circumstances is incidental to the purpose for which the outside entity engages in a contract.

The SHCC may disclose PHI to a BA only to help the SHCC carry out its health care functions—not for the BA’s independent use or purposes. The BA may carry out these functions so long as the SHCC enters into the University’s BA agreement (BAA) or amendment and obtains documented satisfactory assurance that the BA will appropriately safeguard the PHI. The University has determined that in order to simplify compliance with these requirements, the SHCC may enter into agreements with business associates rather than individually amend each and every contract and, where appropriate, the Board of Regents will enter into a single agreement with the vendor or contractors corporate entity rather (e.g., with national accrediting organizations that are the SHCC’s BA for health care operation accreditation purposes).

DHHS has no statutory authority to hold BA liable under the Privacy Rule unless the BA is also a covered entity. When the BA is a pharmaceutical, the federal government may be able to take action under other federal law or agencies, such as the FDA, when the entity has violated the BAA.

**IDENTIFYING THE BUSINESS ASSOCIATE RELATIONSHIP AND WHEN A BUSINESS ASSOCIATE AGREEMENT (BAA) IS REQUIRED**
There has been ongoing confusion amongst covered entities, their contractors and vendors and others within the “HIPAA environment” as to what qualifies as a BA Relationship and when a BAA is required. A BA is an entity that does something for or on behalf of a covered entity—i.e., something the covered entity would have normally done for itself, but has hired someone else to do using PHI.

In many cases, entities are entering into BAA when there is no Privacy Rule defined BA Relationship, thus creating legal requirements and risks when none is mandated under the Privacy Rule. For example, no BAA is required for exchanges of PHI between covered or non-covered providers for treatment purposes.

If an entity is not a HIPAA-covered entity, then a relationship with contractors or vendors is not a HIPAA-defined Business Associate Relationship. No BAA is required. For example, UC has interpreted the Privacy Rule to state that research is not a covered function. Therefore, entities that provide business services to researchers who may use health information are not BA of the researchers because researchers are not themselves covered entities for purposes of carrying out the research protocol.

The HIPAA Taskforce has advised all covered entities within the SHCC to carefully analyze or seek advice from Counsel, the University Privacy Officer or local Privacy Liaison when in doubt regarding whether or not a relationship is a BA Relationship requiring a BAA

Business associate functions and activities include:

1. Payment or health care operations;
2. Claims processing or administration;
3. Data analysis, processing or administration;
4. Utilization review;
5. Quality assurance;
6. Billing;
7. Benefit management;
8. Practice management; or
9. Repricing.

Business associate services include:

1. Legal;
2. Actuarial;
3. Accounting;
4. Consulting;
5. Data aggregation;
6. Management and administrative;
7. Accreditation; and

Relationships that are BAs:

1. A firm that creates a limited data set or deidentifies data, including the entity that is the recipient who receives the limited data set and the data use agreement is combined with the BAA;

2. If the SHCC is performing a function on behalf of, or providing services to, a health plan (e.g., case management services);

3. A firm whose accounting services for SHCC involve access to PHI;

4. Outside counsel whose legal services involve access to PHI;

5. A consultant that performs utilization reviews for the medical center;

6. A Third Party Administrator (TPA) that assists a health plan with claims processing;

7. An independent medical transcriptionist who provides transcription services to a physician;

8. A software company that hosts the software containing PHI on its own server or accesses PHI when troubleshooting the software function, except when the employee of an outside vendor has his or her primary duty station on-site at the SHCC, the SHCC may choose to treat the employee as a workforce member, rather than BA;

9. A pharmacy benefits manager that manages a health plan’s pharmacist network;

10. An accreditation organization

11. A service that provides routine handling of records or shredding of documents containing PHI (as different from a janitorial service) unless the work is under the direct control of the SHCC, when it can be considered a part of the workforce

**RELATIONSHIPS THAT ARE NOT BUSINESS ASSOCIATE RELATIONSHIPS**

The following situations, among others, are not BA relationships and do not require a BAA:

---


81 As distinct from a health plan-provider relationship that is between two covered entities for payment purposes and is not a BA relationship
1. Treatment Uses and Disclosures. Disclosures by the SHCC to an outside health care provider (covered or non-covered) for treatment;\textsuperscript{82}

2. Payment Disclosures between Covered Entities. When a provider discloses PHI to a health plan for payment purposes or when the provider accepts a discounted rate from the plan—each is acting on its own behalf as a covered entity;

3. Incidental Disclosures that Could Not be Reasonably Prevented. With persons or organizations where any access to PHI by such persons would be incidental, if at all, and occurs as by-product of their duties and could not reasonably be prevented (e.g., janitorial or electrician services, plumbers, photocopy repair technicians);

4. PHI Couriers. With a person who is a conduit of or carrier for PHI (private couriers and their electronic equivalents);

5. Software vendors. With an individual or entity who does not need to access PHI in order to provide the vendor service.

6. OHCAs. Among covered entities who participate in an organized health care arrangement (OHCA); and

7. Researchers. To disclose PHI to a researcher for research purposes;\textsuperscript{83}

**BUSINESS ASSOCIATE AGREEMENT/AMENDMENT ELEMENTS**

In general, the SHCC’s Business Associate Amendment (BAA) must contain the elements specified at 45 CFR 164.504 (e) and:

1. Describe the permitted and required uses of PHI by the BA;

2. Provide that the BA will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;

3. Require the BA to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the BAA.

**SHCC AND BUSINESS ASSOCIATE RESPONSIBILITIES WITH RESPECT TO PATIENT RIGHTS**

The SHCC must meet all its responsibilities with respect to an individual’s rights, including the rights of access, accounting and amendment, even when all or a part of the designated record set is held by the BA. The SHCC must specify in the BAA that the BA must make such PHI available when the SHCC must do so to respond to an individual’s rights.

\textsuperscript{82} For example: a hospital lab is not required to have a BAA with a reference lab for treatment purposes

\textsuperscript{83} OCR Privacy Rule December 2002 Guidance, “The researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the BA functions,” page 43
BUSINESS ASSOCIATE TRANSITION PERIOD

Although the Privacy Rule provides for a transition period to April 2004 for those contracts existing prior to October 2003. However, the “transition provisions do not relieve the covered entity of its obligations with respect to PHI held by a business associate,” including an individual’s rights to access or amend PHI held by a BA or receive an accounting of disclosures by a BA. Moreover, to the extent that it is known by the SHCC, the SHCC is responsible for mitigating any harmful effects of unlawful uses and disclosures by the BA. Therefore, the HIPAA Taskforce and the Office of the General Counsel have recommended that all BA be required to amend current and new contracts in order to meet the compliance date of April 2003.

POLICY SIXTEEN IMPLEMENTATION POLICIES

Implementation Policy 16-1

Where the SHCC knows of a material breach or violation of the BAA by the BA, the SHCC is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract. If termination is not feasible, the SHHC is required to report the problem to DHHS Office of Civil Rights.

Implementation Policy 16-2

The Privacy Rule provides for a transition period in order to reduce the regulatory burden for covered entities. If the SHCC has an existing written contract prior to the October 2002 (the effective date of this modification) and does not renew the existing contract prior to April 2003, the Privacy Rule allows the SHCC until April 2004 to enter into a BAA. However, the Office of the General Counsel has recommended that all BA be required to enter into BA agreements or amend contracts prior to April 14, 2003 because the SHCC must be assured that the BA is safeguarding the PHI.

Implementation Policy 16-3

When an individual is seeking credentialing in order to be admitted to the medical staff and those activities require the physician to provide medical records to the medical staff or others, these activities are a part of the SHCC’s operations and not subject to a BAA.

Implementation Policy 16-4

The SHCC must enter into BAA with accreditation organizations or enter into a Data Use Agreement in order to provide a Limited Data Set for those accreditation purposes. In most cases, the SHCC should enter into a single system BAA with the accreditation organization.

Implementation Policy 16-5

The University of California is a governmental entity and if the SHCC has a business associate relationship with another governmental entity for purposes other than treatment (no BAA is

84 Final Privacy Rule Preamble, 162 of 216
required for treatment purposes), the requirements of the business associate amendment may be met by:

1. Entering into a Memorandum of Understanding with the governmental entity; or
2. Determining if current state or federal law requires that the governmental entity/business associate comply with regulations that meet the objectives of the HIPAA Privacy Rule Business Associate Standard.

The University’s Office of the General Counsel will provide the SHCC with a legal opinion as to whether an MOU is necessary in those situations where the University has a business associate relationship with another governmental entity. The University’s Privacy Officer will document those determinations.

**Implementation Policy 16-6**

When UC workforce members perform business associate type functions the SHCC, no BAA is required because in those situations, the workforce members are part of the SHCC’s workforce and are subject to all the HIPAA Privacy Rule requirements and the University’s policies.

**Implementation Policy 16-7**

The Privacy Rule does not require a business associate contract for disclosure of PHI from a group health plan to a plan sponsor. The group health plan can disclose PHI to a plan sponsor if, among other requirements, the plan documents are amended to appropriately reflect and restrict the plan sponsor’s uses and disclosure of such information.

**Implementation Policy 16-8**

There may be situations when SHCC volunteers or contracted individuals have access to PHI that would be limited, incidental to the purpose of their job, and limited in nature and no BA relationship exists (e.g., when outside entities take newborn photos or clowns entertain children in the University’s Children’s Hospitals). To provide reasonable safeguards, the SHCC covered institution or entity should:

1. Require that those outside entities or persons sign a confidentiality agreement and receive information regarding the Privacy Rule; or
2. Require HIPAA training when those activities are carried out by the SHCC’s volunteers and SHCC workforce members.

---

85 In those cases where the University is a plan sponsor or acting as the employer, the University does not need to negotiate a business associate amendment with the group health plan or provide the employee’s authorization in order for the health plan to respond to questions posed by the University’s benefit managers or others representing the interests of the employee, so long as the plan documents have been amended accordingly.
**Implementation Policy 16-9**

The SHCC may contract with the BA to provide the point of contact for individuals to request an amendment or accounting of disclosures of PHI. In such a case, the BAA should require the BA to provide all necessary documentation to the SHCC as required for reporting and record keeping.

**Implementation Policy 16-10**

The SHCC is not liable for the privacy violations of a BA, nor does it need to actively monitor or oversee the BA compliance. The BA must notify the SHCC of a violation. If the SHCC is aware of a violation, the SHCC must take action to remedy the violation. In extreme cases, the SHCC may have to terminate the contract and/or notify DHHS.

**Implementation Policy 16-11**

SHCC workforce must report suspected violations of the BAA by the BA to the appropriate persons within the SHCC, including Counsel, University Privacy Official, or local Privacy Officer or Liaison.

**Standard Seventeen: Documentation Requirements**

CFR 164.530

**Implementation Policy 17-1:**

The SHCC must maintain the policies and procedures required by the Privacy Rule, including the System Standards in written or electronic form for six year. A copy of the System Standards may be access at the University’s HIPAA Website at: [www.universityofcalifornia.edu/hipaa](http://www.universityofcalifornia.edu/hipaa) or by contacting the University Privacy Official at the address on the Web-site or the University of California Office of the President, Office of the Senior Vice President of Business and Finance.

**Implementation Policy 17-2: Required Documentation**

The Privacy Rule requires the SHCC to document and retain for six years the documentation of the following:

1. Business Associate Agreements—document and maintain copies of all Business Associate Agreements;

2. Authorizations—document and maintain copies of all signed Patient Authorizations and document that there has been verification of the person’s right to sign on behalf of the patient;

3. Waiver of Authorizations for Research Purposes—document certification from the researcher requesting PHI that the IRB has approved a Waiver of Authorization and met the HIPAA-required criteria for a Waiver of Authorization;
4. Notice of Privacy Practices—maintain copies of the Notice, written acknowledgements of receipt, and good faith effort to obtain written acknowledgement when patient refuses to provide written acknowledgement;

5. Restrictions on practices described in the Notice—document any agreed to restrictions;

6. Access or copying of the DRS—document the DRS that is subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access by individuals; document responses to requests for access or copying as required;

7. Amendment—document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals; document responses to request for an amendment as required;

8. Accounting—document the information required to be in an accounting (see 164.503 (j); the written accounting that is provided to the individual; titles of the persons or offices responsible for receiving and processing requests for an accounting; statement of the law enforcement or health oversight agency or official (if made orally) who has requested that the SHCC temporarily suspend accounting because it could impede the agency’s activities; document responses to request for an accounting as required;

9. Personnel Designations—document the privacy official and contact person or office who is responsible for receiving complaints;

10. Training—document that the SHCC has provided training to all members of the workforce on the policies and procedures as necessary and appropriate for the members to carry out their function within the covered entity;

11. Complaints—document all complaints received and their disposition, if any;

12. Sanctions—document any sanctions that are applied against members of the workforce who fail to comply with the privacy policies and procedures of the SHCC;

13. Changes to policies and procedures or privacy practices as described in the Notice—document any changes to policies and procedures prior to the effective date of the change and make appropriate changes to the Notice; and

14. SHCC’s HIPAA Policies and Procedures—document system and local policies and procedure.

**Implementation Policy 17-3: Recommended Documentation**

While not specifically required in the Privacy Rule, the SHCC has determined that it is in the best interest of the patient, the member and UC to retain documentation for the following (note: HIPAA requires that the covered entity provide written responses in all of the following circumstances but does not require the patient or member to provide a written requests):

1. Data Use Agreements;

2. Verifications of identity of public officials requesting information;
3. Patient written requests for Restrictions;

4. Patient written request for access to or copies of the DRS, SHCC response to the patient’s request, written denial of the request, written statement of the reason for a delay in taking timely action on the request, written rebuttal statement, and any other written actions;

5. Patient written request for amendments to PHI, SHCC’s written denial of the amendment, written statement for reasons for delay in responding to requests, patient’s written statement disagreeing with the denial of the amendment, SHCC’s written rebuttal;

6. Patient written requests for an accounting, written statement for reasons for delay in responding to requests;

7. Patient written request for confidential communications of PHI and SHCC response;

8. SHCC’s training materials;

9. Accounting—when a law enforcement or health oversight agency has submitted a written request to temporarily suspend accounting, the SHCC should document the written request;

10. Notification of victims of abuse, neglect or domestic violence—notify the individual of any disclosures to governmental agencies or, if the professional determination has been made not to notify the individual or individual’s personal representative, document why;

11. Permitted disclosures for judicial and administrative proceedings—documentation required from a party seeking PHI in a judicial or administrative proceeding should be maintained by the SHCC; and

12. Researcher’s request for decedent information—SHCC may request documentation from researcher of death of subject.
Appendix A: Members of the SHCC’s HIPAA Taskforce

The following is a list of the members of the SHCC’s system-wide HIPAA Taskforce as of April 14, 2003. Those names that are starred (*) are the campus or academic health center designated Privacy Officers or Liaisons to the Taskforce.

NOTE: I will send out this Appendix after we reconfirm the 100 plus titles for everyone.

Appendix B: The University’s HIPAA Implementation Packet

The following is a list of those documents that have been created and implemented by the SHCC HIPAA Taskforce and responsible individuals at each of the covered entities within the SHCC. Copies of the documents may be obtained on the University’s HIPAA Website at: www.universityofcalifornia.edu/hipaa.

1. Notice (s) of Privacy Practices
   a. Medical
   b. Mental Health and Behavioral Health
   c. Self-Funded Health Plans
   d. Sample Written Acknowledgement Form

2. Business Associate Agreement

3. Training Modules
   a. HIPAA 101
   b. Provider
   c. Research
   d. PHI Management
   e. Institutional Advancement, Media and External Relations
   f. Human Resources and Benefits
   g. UCOP
   h. Other

4. Authorization Form (s)
   a. Basic Boxed Version
   b. Basic Unboxed Version
c. Institutional Advancement, Media, External Relations

d. Marketing

e. Research

5. Forms for an Individual to Use When Exercising Privacy Rights

   a. Restriction

   b. Confidential Communication

   c. Amendment

   d. Accounting of Disclosures

   e. Access and Copying