

**FINAL HIPAA**  
**PRIVACY**  
**REGULATIONS**

**BJC HEALTHCARE**  
**REVISED SUMMARY**

**FINAL HIPAA PRIVACY REGULATIONS**

**BJC HEALTHCARE SUMMARY**

**Table of Contents**

Introduction ..... 1

Definitions ..... 1

Relationship of the Privacy Regulations to Other State and Federal Laws ..... 6

Compliance, Enforcement, and Sanctions ..... 6

Verbal Agreements and Authorizations for the Use or Disclosure of PHI ..... 6

    Authorizations ..... 7

        Specific circumstances in which an authorization is necessary ..... 7

        Specific circumstances in which an authorization is *not* necessary ..... 7

        Authorization requirements ..... 7

        Compound authorizations ..... 8

        Treatment or Payment contingent upon Individual signing an authorization .... 9

        Revocation of authorizations ..... 9

    Verbal agreements. .... 9

        Verbal agreement requirements ..... 9

        Facility Directories ..... 10

        Persons involved in the Individual’s Treatment ..... 10

        No requirement to verify the identity of persons ..... 11

    When a Covered Entity *may* Disclose PHI without a verbal agreement or authorization  
        ..... 11

        Treatment, Payment or Health-Care Operations (“TPO”) ..... 11

        Incidental Uses and Disclosures ..... 12

        Public health activities ..... 12

        Victims of abuse, neglect, or domestic violence ..... 13

        Health oversight activities ..... 13

        Judicial or administrative proceedings ..... 13

        Law enforcement purposes ..... 14

        Crime victims ..... 15

        Deaths ..... 16

        Coroners, medical examiners (“MEs”), and funeral directors ..... 16

        Organ procurement/donation ..... 17

        Aversion of serious threats to the health or safety of a person or the public .... 17

        Military personnel ..... 17

        Inmates ..... 17

        Workers’ Compensation ..... 17

When a Covered Entity is *required* to Disclose PHI ..... 19

Affiliated Entities and Business Associates .....	19
Research .....	19
Business Associates .....	22
Existence of a Business Associate relationship .....	22
Business Associate contracts .....	22
Individuals’ Rights Under the Privacy Regulations. ....	24
Individuals have five enumerated rights .....	24
The right to notice of the Covered Entity’s privacy practices for PHI .....	24
The right to request privacy protections, including the right to restrict Uses or Disclosures and the right to designate methods for confidential communications	27
The right of access to PHI .....	28
The right to request an amendment of PHI .....	31
The right to an accounting of Disclosures of PHI .....	34
Marketing and Fund-raising Activities .....	37
Marketing .....	37
Fund-raising .....	38
Administrative Requirements .....	38
Privacy personnel .....	38
Privacy policies and procedures .....	38
Privacy training .....	39
Privacy safeguards .....	39
Privacy complaints .....	39
Privacy sanctions and mitigation .....	39
No intimidation or retaliation .....	39

# **FINAL HIPAA PRIVACY REGULATIONS**

## **BJC HEALTHCARE SUMMARY**

### **I. Introduction.**

The following is a summary of the final Standards for Privacy of Individually Identifiable Health Information released by the Department of Health and Human Services (“HHS”) on December 28, 2000 and August 14, 2002 (collectively, the “Privacy Regulations”). Congress enacted the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) that, in part, authorized HHS to promulgate the Privacy Regulations as a means by which the federal government can regulate the disclosure and use of certain individually identifiable health information (so-called Protected Health Information or “PHI”). The Privacy Regulations will have a significant impact not only on BJC HealthCare and its affiliated hospitals and physicians, but also on BJC’s self-funded health plans and certain vendors with which it conducts business. BJC must be in compliance with the Privacy Regulations’ rules and standards no later than April 14, 2003.

This Summary has been prepared by the BJC HIPAA Steering Committee, which is a collaborative effort of BJC Legal Services, Risk Management, Audit Services, and Information Services. In reading this Summary, keep in mind that it is intended to serve only as a synopsis of the major rules and standards against which BJC will need to analyze its current operations to determine what measures are necessary to ensure compliance with the Privacy Regulations.

### **II. Definitions.**

Below are definitions for terms that appear in the Privacy Regulations and that are used throughout this Summary. You should briefly review this Section before continuing on with the rest of the Summary and then refer back to it when you are in doubt as to the meaning of a specific term. In particular, the following terms are referenced quite frequently: Covered Entities, PHI, Business Associate, Use, and Disclosure. For your convenience, defined terms (and derivatives thereof) are capitalized throughout the Summary.

Affiliated Entities – legally distinct Covered Entities that share a Common Ownership or Control and that may designate themselves as a single Covered Entity for purposes of the Privacy Regulations. All hospitals that are member entities of BJC HealthCare will be treated as Affiliated Entities for purposes of the Privacy Regulations.

Business Associate - any person or organization who, on behalf of BJC, either: (i) performs or assists in the performing of (a) any function or activity involving the Use or Disclosure of PHI, such as claims processing or administration, utilization review, quality assurance billing, benefit management, practice management, and repricing, or (b) any other function or activity subject to regulation under the Privacy Regulations; or (ii) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for BJC if the provision of services of services involves the Disclosure of PHI from BJC (or from another Business

Associate of BJC). Notwithstanding the foregoing, the term “Business Associate” does not include any member of BJC’s Workforce.

Common Control - Common Control exists if any entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity.

Covered Entities – (i) Health Care Provider(s) who transmit any PHI in electronic form; (ii) Health Plan(s); and (iii) Health-Care Clearinghouse(s).

Data Aggregation - data collected by a Business Associate from a Covered Entity and combined with the PHI of one or more Covered Entities to permit data analysis of the Health-Care Operations of the respective Covered Entities.

Designated Licensed Health-Care Professional or “L.P.” - the person designated by a Covered Entity who is a licensed health-care professional and who will not participate in any initial decisions to deny or grant access to PHI, but, rather, will review all requests for access denied on reviewable grounds as established by the Privacy Regulations. The Designated L.P. may be the Chief Nurse Executive, the Chief Medical Officer, or a Medical Director.

Designated Record Set – (i) for BJC Health-Care Providers, any record used, in whole or in part, to make decisions about Individuals, including (a) medical records (such as admission data, physician notes, nursing forms, medication records, nutrition notes, test and lab reports, dictated reports of operation, advance directives and expiration documents, but excluding release forms, correspondence, peer review files, explanation of benefits, remittance advices, and volunteer donors of blood and blood products information) and (b) billing records (such as itemized statements, Medicare/Medicaid standard forms, claim forms) held or maintained by or for a Health Care Provider for the applicable retention period, (ii) for BJC Health Plans, records used to make decisions affecting Individuals (such as enrollment, payment, claims, and medical management records).

Direct Treatment Relationship - a Treatment relationship that involves direct patient contact and/or communication.

Disclosure - divulging PHI, in any manner, outside of the Covered Entity creating or possessing the PHI.

Facility Directory - a patient’s name, location in the facility (except for inpatient psychiatric patients), and/or the general health condition of the patient.

Health Care - the care, services, or supplies (including prescription drugs and durable medical equipment) related to an Individual’s health.

Health-Care Clearinghouse - a public or private entity that processes, or facilitates the process of, PHI in a non-standard format (or containing non-standard data elements) into standard data elements or a standard transaction, and vice-versa. In other words, a

Health-Care Clearinghouse receives health care transactions from Health-Care Providers or other entities, and translates the data from a given format into one acceptable to the intended payor(s). Most commonly, Health-Care Clearinghouses are organizations that facilitate the electronic submission of claims to insurance companies and HMOs on behalf of Health-Care Providers.

Health-Care Operations – the activities of a Covered Entity that cause it to be categorized as a Health-Care Provider, Health Plan, or Health-Care Clearinghouse. Such activities include, but are not limited to, the following: (i) quality assessment and improvement (QA/QI); (ii) outcomes evaluation; (iii) development of clinical guidelines; (iv) protocol development; (v) case management and care coordination; (vi) communication with providers and patients about treatment alternatives; (vii) review of competence or qualifications of health professionals; (viii) training programs for students and practitioners; (ix) provision of legal services; (x) fraud and abuse auditing and compliance programs; (xi) business planning and development, management, and administration; (xii) Fund-raising for the benefit of the Covered Entity; (xiii) marketing for which an authorization is not received; and (xiv) due diligence functions.

Health-Care Provider - a provider of health care (e.g., physician, hospital) that furnishes, bills, or is paid for Health Care in the normal course of business.

Health Insurance Issuer - an entity licensed to conduct insurance business that is regulated by state law, excluding self-funded plans.

Health Oversight Agency - an agency authorized by law to oversee the health-care system or government programs for which PHI is necessary to determine eligibility for or compliance with the government program, or is necessary to enforce civil rights laws. For example, HHS, the Centers for Medicare and Medicaid Services (formerly, HCFA), state insurance commissions, state health professional licensure agencies, Officers of Inspectors General of federal agencies, the Department of Justice, state Medicaid fraud control units, OSHA and the FDA are considered Health Oversight Agencies.

Health Plan - an individual or group plan that provides or pays for the cost of medical care, including group health plans, health insurance issuers (including insurance companies), HMOs, the Medicare and Medicaid programs, an issuer of Medicare supplemental insurance, CHAMPUS, TriCare, the Indian Health Service Program, Federal Employee Health Benefits Program (“FEHBP”), an approved State Children’s Health Insurance Program (“SCHIP”), a high risk pool established under state law, an issuer of a long-term care policy, and a multiple-employer plan. Health Plans do not include any plan that pays for excerpted benefits and is a government-funded program, if the government-funded program’s principal activity does not involve providing or paying for Health Care or the principal activity is the direct provision of Health Care or the making of grants to fund Health Care. Examples of such excluded programs include the Food Stamp Program, the Special Supplemental Nutrition Program for Women, the Ryan White Comprehensive AIDS Resources Emergency Act, and the government-funded health care centers and immunization programs (except that some of the programs may meet the definition of a Health-Care Provider). The fact that a local welfare agency

simply determines eligibility or enrollment in a Health Plan is not sufficient in and of itself to make such an agency a Health Plan.

Identifier – a piece of information that, alone or in combination with other pieces of information, enables identification of an Individual (e.g., name, address, date of birth, telephone number, VIN, certificate/license numbers, etc.).

Indirect Treatment Relationship - a relationship between a Health-Care Provider and an Individual in which the Health-Care Provider delivers Health Care to the Individual at the direction (i.e., by order) of another Health-Care Provider and the Health-Care Provider usually provides the services or reports the diagnoses to the ordering Health-Care Provider who in turn delivers the services or reports to the Individual. For example, in some cases, this type of relationship would include radiology or laboratory services in which reports and diagnoses are provided to the ordering Health-Care Provider.

Individual - the person who is the subject of PHI or that person's personal representative. If the person is an adult and state law permits, the "personal representative" can be a court-appointed guardian or power of attorney. If the person is an unemancipated minor, the "personal representative" can be the parent or guardian or person acting *in loco parentis*. If the minor can consent on his or her own behalf under state law, the minor is considered to be emancipated for purposes of the Privacy Regulations. If the person is a deceased patient, the "personal representative" can be the executor, administrator, or other person allowed to act on behalf of the deceased patient's estate.

Inmate - a person who is confined in a correctional institution, such as a prison, jail, reformatory, work farm, detention center, home detention or halfway house.

Marketing – a communication about a product or service by a Covered Entity that encourages recipients of the communication to purchase or use the product or service, although certain exceptions apply (see Section VIII, below), or an arrangement between a Covered Entity and any other entity whereby the Covered Entity Discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliates to make a communication about its own product or service that encourages recipients of the communication to purchase or use the product or service.

Organized Health-Care Arrangement - (a) a clinically integrated setting where Health Care is provided by more than one Health-Care Provider; or (b) an organized system of Health Care in which more than one Covered Entity (i) holds itself out to the public as participating in a joint arrangement and (ii) participates in at least one specified joint activity either for each other or by a third party on behalf of each other.

Payment – (i) activities undertaken by a Health Plan to collect premiums or determine benefits under the Health Plan; (ii) activities undertaken by a Health-Care Provider in order to obtain reimbursement for Health Care services; or (iii) any of the following activities: determining eligibility and adjudicating and subrogating claims; risk adjusting amounts due based on health status and demographics; billing, claims management, collection or obtaining payment under a reinsurance contract, and related

data processing; reviewing PHI with respect to medical necessity or justification of charges; utilization review (UR) activities; or Disclosure to consumer reporting agencies for collections.

Privacy Regulations - the Standard for Privacy of Individually Identifiable Health Information issued by the Department of Health and Human Services (65 Fed. Reg. 82462 et seq. (December 28, 2000) and 67 Fed. Reg. 53182 et seq. (August 14, 2002)), as may be amended from time to time.

Protected Health Information (“PHI”) - information that was created or received by a Covered Entity and has been transmitted in any form or medium (i.e., electronically, on paper, or orally). Further, the information must concern (a) an Individual’s physical or mental condition, (b) the provision of Health Care to an Individual, or (c) the Payment for the provision of Health Care to an Individual. Finally, the information must either identify the Individual or create a reasonable basis to believe that the information (including demographic information) can be used to identify the Individual.

Psychotherapy Notes - notes kept by a mental health professional that analyze conversations during a counseling session and that are separated from the rest of the Individual’s medical record.

Public Health Authority – an agency or authority of the U.S., a state, territory, or Indian tribe that is responsible for public health matters as part of its official mandate. Includes a person or entity acting under a grant of authority from, or contract with, a public health agency; for example, State, City or County departments of health and the Centers for Disease Control and Prevention.

Research - the systematic investigation (including research development, testing, and evaluation) designed to develop or contribute to generalized knowledge. Research is not considered to be TPO nor should Research be considered a performance improvement activity.

Secretary - the Secretary of the Department of Health and Human Services or his or her designee.

Single Affiliated Covered Entity - legally separate Covered Entities that are under common ownership or common control. Common ownership is an ownership or equity interest of five percent or more in another entity. Common control is the power, directly or indirectly, to significantly influence or direct the actions of policies of another entity.

TPO - An abbreviation commonly used to collectively refer to Treatment, Payment, or Health-Care Operations.

Treatment - (i) the provision, coordination, or management of Health Care and related services by one or more Health-Care Providers, including coordination with a third party; (ii) consultation between Health-Care Providers concerning an Individual; or (iii) the referral of a patient by one Health-Care Provider to another.

Use - the sharing, employment, application, utilization, examination, or analysis of PHI.

Workforce – any BJC employee, volunteer, trainee, or other person whose conduct, in the performance of work for BJC, is under BJC’s direct control whether or not they are paid by BJC. Students in training at BJC-affiliated hospitals are considered to be a member of BJC’s Workforce.

### **III. Relationship of the Privacy Regulations to Other State and Federal Laws.**

The Privacy Regulations establish a “federal floor” for the protection of PHI. Consequently, the Privacy Regulations make room for state laws that regulate information falling within the definition of PHI and that are “more stringent” than a corresponding provision of the Privacy Regulations. In the coming months, we will be analyzing Missouri and Illinois law to determine to what extent these two states have laws that are either contrary to, or “more stringent” than, the Privacy Regulations’ rules and standards. In addition, we will examine pertinent federal laws that have already established standards or rules that are potentially in conflict with those of the Privacy Regulations. Once these analyses have been completed, a follow-up memorandum to this Summary will be circulated.

### **IV. Compliance, Enforcement, and Sanctions.**

Violations of the Privacy Regulations carry civil and criminal penalties, including imprisonment. HHS has delegated to its Office of Civil Rights (“OCR”) the specific oversight authority of compliance with the Privacy Regulations. The OCR has the authority to receive and investigate complaints against a Covered Entity for alleged violations of the Privacy Regulations. Any person, not just an Individual, may file such a complaint with the OCR. Upon request, Covered Entities must provide the OCR with access to their facilities and records and submit compliance reports as necessary for the OCR to determine if they are in compliance with the Privacy Regulations. Additionally, in certain circumstances, the OCR will be entitled to access a Covered Entity’s facilities and records *without* any prior notice.

The Privacy Regulations do not specifically allow Individuals to sue Covered Entities for violations. It is likely, however, that civil suits will begin asserting the theory that a violation of the Privacy Regulations constitutes negligence. If successful, such a claim may be sufficient to permit the Individual to recover damages.

### **V. Verbal Agreements and Authorizations for the Use or Disclosure of PHI.**

This Section of the Summary addresses the question that lies at the heart of the Privacy Regulations: In what circumstances, if any, can a Covered Entity Use or Disclose PHI? A Covered Entity may use or disclose PHI without an Individual’s Authorization or Verbal Agreement if the Use or Disclosure of PHI is made in furtherance of TPO, or if the Use or Disclosure is required under law.

- A. Authorizations. For Disclosures of PHI not otherwise required or permitted under the Privacy Regulations, a Covered Entity must obtain a specific, written authorization from an Individual before Using or Disclosing his or her PHI.

1. Specific circumstances in which an authorization is necessary. The following is a list of common situations in which an authorization is necessary: (i) Marketing practices (see Section VIII, below); (ii) employment determinations; (iii) Fund-raising (see Section VIII, below); and (iv) Psychotherapy Notes, even if the Disclosure or Use is for TPO.
2. Specific circumstances in which an authorization is *not* necessary. The following is a list of common situations in which an authorization is unnecessary: (i) Psychotherapy Notes needed for “oversight” activities/investigations into the Health-Care Provider; (ii) Disclosures to HHS for enforcement or compliance purposes; (iii) Disclosures mandated by law; (iv) Disclosures to prevent a serious threat to the health or safety of another person or the public; (v) Disclosures to the Individual herself or himself; or (vi) Disclosures for the purpose of TPO.
3. Authorization requirements.
  - a. Basic requirements. In order to be valid, an authorization must:
    - (1) be written in plain language and signed and dated by the Individual (or, if signed by the Individual’s representative, it must additionally state that person’s authority or relationship to the Individual);
    - (2) clearly describe the PHI to be Used or Disclosed;
    - (3) name the Covered Entity or class of entities or persons authorized to make the Use or Disclosure;
    - (4) name the recipients or list the types of recipients;
    - (5) indicate the authorization’s expiration date (can be a specific date or a specific time period or event period directly relevant to the Individual or the purpose for the Use or Disclosure);
    - (6) state that the Individual has the right to revoke the authorization, including instructions as to how and where the Individual can complete such a revocation (or a referral to the Covered Entity’s notice of privacy practices (see Section VII.B, below));
    - (7) state that the PHI, once it is Used or Disclosed pursuant to the authorization, may no longer be protected by the Privacy Regulations.

- (8) state that the Covered Entity cannot condition Treatment, Payment, enrollment, or eligibility on the Individual agreeing to sign the authorization, and if conditioning is permitted, then state any consequence to the Individual for refusing to sign the authorization (for example, BJC may condition the provision of Research-related Treatment upon receipt of a signed authorization from the Individual);
- (9) identify each purpose for which the PHI is to be Used or Disclosed as well as the specific PHI that will be Used or Disclosed (i.e., broad or blanket authorizations are *not* permitted);
- (10) state that the Covered Entity will receive direct or indirect remuneration from a third party in exchange for the Use or Disclosure of the PHI, if the Covered Entity will indeed receive such remuneration; and
- (11) state that the Covered Entity has provided the Individual with a signed copy of the authorization.

4. Compound authorizations.

- a. General rule. An authorization cannot be combined with (i) the Covered Entity's notice of privacy practices (see Section VII.B, below), (ii) an informed consent for Research purposes, (iii) any other form of consent or authorization for Treatment or Payment purposes, or (iv) any other form of written legal permission for Use or Disclosure of PHI.
- b. Exceptions. An authorization can be combined with another form of valid permission in the following situations:
  - (1) An authorization for Use or Disclosure of PHI created for Research purposes may be combined with any other type of written permission for the same Research study, including another authorization for the Use or Disclosure of PHI for such Research or a consent to participate in the Research.
  - (2) An authorization for Use or Disclosure of Psychotherapy Notes for multiple purposes may be combined into a single authorization.
  - (3) Authorizations for the Use or Disclosure of PHI may be combined if the Covered Entity has not conditioned Treatment, Payment, eligibility, etc. upon the Individual's signing any of the relevant authorizations.

5. Treatment or Payment contingent upon Individual signing an authorization. In general, a Covered Entity is prohibited from conditioning Treatment or Payment upon an Individual signing an authorization except if the Use or Disclosure for which the authorization is sought does not pertain to Psychotherapy Notes and is for:
    - a. Research purposes;
    - b. an Individual who is to be given Treatment at the Covered Entity for the sole purpose of providing information to a third party (e.g., insurance application pre-screening examinations); or
    - c. the purpose of determining eligibility for enrollment (if the Covered Entity is a Health Plan) or the Health Plan's underwriting or risk rating determinations.
  6. Revocation of authorizations. Individuals can revoke their authorizations at any time, in writing, except (i) if the authorization was obtained as a condition of the Individual receiving insurance coverage or (ii) to the extent that the Covered Entity has taken action in reliance upon the authorization.
- B. Verbal agreements. In addition to authorizations, the Privacy Regulations also permit Covered Entities to obtain "verbal agreements" from Individuals for the limited purposes of Disclosing PHI for Use in Facility Directories and for Disclosing PHI to persons assisting in the Individual's care (e.g., family members, close friends).
1. Verbal agreement requirements. In order for the verbal agreement to be valid, Health Care Providers must inform the Individual in advance of the intended Use or Disclosure and provide a meaningful opportunity for the Individual to prevent or restrict the Use or Disclosure. In exceptional circumstances, however, a Health Care Provider can make a decision based upon his or her professional judgment as to what is in the Individual's best interest, such as if the Individual is unconscious and requires emergency Treatment.
  2. Facility Directories.
    - a. General rule. A Health Care Provider can only include PHI about a specific Individual in its Facility Directory if (i) it informs (verbally or in writing) all Individuals of the Health-Care Provider's policies regarding the Facility Directory; (ii) it provides a meaningful opportunity for the Individual to opt out or to restrict some or all of the PHI that is included in the Facility Directory; and (iii) the Individual informs (verbally or in writing)

the Health-Care Provider that he or she does not object to being included in the Facility Directory.

- b. What PHI can be listed in the Facility Directory for Disclosure to third parties. Subject to the Individual's right to object or the Individual's known, prior express preferences, Health-Care Providers may Disclose the following PHI to persons who inquire about the Individual *by name*: (i) the Individual's general condition in terms that do not communicate specific medical information about the Individual (i.e., fair, critical, stable, etc.); and (ii) the Individual's location in the facility (e.g., ICU, maternity, etc.). Without the Individual's verbal agreement, the foregoing PHI can only be disclosed if (a) the Individual is incapacitated, or (b) emergency Treatment is required and, in accordance with the Health-Care Provider's professional judgment, the Disclosure is in the Individual's best interest. Once the Individual is recovered to the extent that he or she can understand what PHI the Health-Care Provider wishes to include in its Facility Directory, the Health-Care Provider must then discuss that information with the Individual and give her or him the opportunity to opt out.
- c. Clergy. For inquiries from clergy, a Health-Care Provider can Disclose the name, general condition, location, and religious affiliation of the Individual.

3. Persons involved in the Individual's Treatment.

- a. General rule. A Health-Care Provider can Disclose PHI to a person involved in the Individual's current Treatment (i.e., a family member or other relative, close personal friend, or other person identified by the Individual).
- b. Individuals with capacity and who are present. In circumstances in which the Individual is present and has capacity, the Health-Care Provider must:
  - (1) obtain the Individual's verbal agreement to Disclose;
  - (2) give the Individual an opportunity to object; and
  - (3) receive no objection from the Individual (or, in certain circumstances, be able to reasonably infer that the Individual has no objection to the Disclosure).
  - (4) Individuals incapacitated or who are not present. If the Individual is not present or is incapacitated, the Health-

Care Provider can Disclose PHI to persons involved in the Individual's current Treatment to the extent that the Health-Care Provider believes, in the exercise of his or her professional judgment, that the Disclosure is in the Individual's best interest. In these circumstances, the Health-Care Provider must only disclose PHI that is directly relevant to the person's involvement with the Individual's Treatment. This rule should be construed narrowly to allow Disclosures only to those persons who have the closest relationships with the Individual and in circumstances in which the Individual cannot consent.

- c. No requirement to verify the identity of persons. The Privacy Regulations do not require Health-Care Providers to verify the identity of persons covered by this rule.

C. When a Covered Entity may Disclose PHI without a verbal agreement or authorization. Covered Entities may (but are not required to) Use or Disclose PHI without an Individual's verbal agreement or authorization in the following circumstances:

- 1. Treatment, Payment or Health-Care Operations ("TPO"): A Covered Entity may Use or Disclose PHI for its own TPO, except for those Uses or Disclosures that require an Authorization (see Section V.A., above). In addition, a Covered Entity may Disclose PHI for Treatment activities of another Health-Care Provider. A Covered Entity may Disclose PHI to another Covered Entity or Health-Care Provider for the Payment activities of the entity that receives the information. A Covered Entity may Disclose PHI to another Covered Entity for the Health-Care Operations of the entity that receives the information, if each entity has or had a relationship with the Individual who is the subject of the PHI, the PHI pertains to such relationship, and the Disclosure is:
  - a. for the purpose of conducting quality assessment and improvement activities or reviewing the competence or qualifications of health care professionals; or
  - b. for the purpose of detecting health care fraud and abuse compliance.

Finally, a Covered Entity that participates in an Organized Health-Care Arrangement may Disclose PHI about an Individual to another Covered Entity which participates in the Organized Health-Care Arrangement for any Health-Care Operations activities of the Organized Health-Care Arrangement.

2. Incidental Uses and Disclosures: An incidental Use and Disclosure of PHI: (i) is a secondary Use or Disclosure that cannot reasonably be prevented; (ii) is limited in nature; and (iii) occurs as a by-product of an otherwise permitted Use or Disclosure. Incidental Uses and Disclosures of PHI, whether or not related to Treatment, are permitted if the Covered Entity applies reasonable safeguards to protect PHI and implements the “minimum necessary” requirements (see Section V.D, below).
3. Public health activities. A Covered Entity can Disclose PHI without a verbal agreement or authorization from the Individual if the Disclosure is to:
  - a. a Public Health Authority authorized by law (including a foreign health agency) to collect or receive information for the purpose of preventing/controlling disease or injury;
  - b. a Public Health Authority in charge of investigating child abuse or neglect;
  - c. a person subject to the jurisdiction of the Food and Drug Administration (“FDA”) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of the activities related to quality, safety or effectiveness of such FDA-regulated product or activity (i.e., collecting or reporting adverse events, product defects or problems, or biological product deviations; tracking FDA-regulated products; enabling product recalls, repairs, replacement or lookback; or conducting post-marketing surveillance);
  - d. a Public Health Authority, if a person has been exposed to a communicable disease or is at risk of spreading a communicable disease and the Covered Entity is authorized by law to notify the Public Health Authority;
  - e. a Public Health Authority for work-related injuries, if the Covered Entity provides notice to the Individual; or
  - f. another government agency, if that government agency is acting at the direction or request of a Public Health Authority.
4. Victims of abuse, neglect, or domestic violence. A Covered Entity can Disclose PHI without a verbal agreement or authorization from the Individual if the Disclosure is to any government authority authorized by law to receive such reports, but *only if* (i) the Individual agrees to the Disclosure; (ii) the Covered Entity is expressly authorized by statute or regulation to Disclose the PHI and the Covered Entity believes that the Disclosure is necessary to prevent serious harm to the Individual or other

persons; or (iii) the Individual is incapacitated and a law enforcement official has informed the Covered Entity that a media enforcement activity depends upon the Disclosure and that waiting for the Individual to regain capacity would materially and adversely affect the campaign.

5. Health oversight activities. Covered Entities can Disclose PHI to Health Oversight Agencies for oversight activities allowed by law without a verbal agreement or authorization. Such oversight activities include, but are not limited to, audits, investigations, and inspections.
6. Judicial or administrative proceedings.
  - a. General rule. Covered Entities can disclose PHI in an administrative/judicial proceeding if the request is made through, or pursuant to, a court order or administrative tribunal or is in response to a subpoena *issued by a court* (not a party) or discovery request form (if the Covered Entity is a party). Absent a court order or a subpoena issued by a court or administrative tribunal, the Covered Entity may respond to a subpoena or a discovery request *only if* the Covered Entity does one of the following:
    - (1) Obtains satisfactory assurances that reasonable efforts have been made to give the Individual whose PHI has been requested notice of the request. “Satisfactory assurances” in this case would consist of (a) a written notice to the Individual’s last known address with sufficient information in the notice concerning the situation and (b) the period of time for objection by the Individual has lapsed without the Individual objecting.
    - (2) Obtains satisfactory assurances that the party seeking the PHI has made reasonable efforts to secure a qualified protective order that will guard confidentiality of the PHI. “Satisfactory assurances” in this case would include a statement and documentation that the parties have agreed to a protective order or that the party seeking the PHI has requested such a protective order from a court. A “qualified protective order” would be a protective order that prohibits the parties from Using or Disclosing the PHI for any purpose other than for the litigation or proceeding for which the PHI is requested. In addition, a “qualified protective order” would require the return to the Covered Entity of the PHI (including any copies) or its destruction when the litigation or proceedings are completed.
    - (3) “Minimum necessary” requirement. If the Covered Entity is *not* required by law to Disclose the PHI, the “minimum

necessary” requirement (see Section V.D, below) applies. If the Disclosure is required by law (i.e., a court order), the “minimum necessary” requirement does not apply, but the Covered Entity should nonetheless only Disclose PHI to the extent that it is within the scope of the permitted Disclosure. In addition, the Covered Entity *may* notify the Individual of the requested Disclosure and permit the Individual to either determine the scope of the Disclosure to the requesting party or seek a protective order from a court.

- b. Reconciling the distinction between Disclosures for health oversight activities and Disclosures for judicial or administrative proceedings. If there is a question as to which rule applies as between the one for health oversight activities and the one for judicial or administrative proceedings, the requested Disclosure should be considered as pertaining to health oversight activities if:
- (1) an Individual is the subject of the investigation or activity; or
  - (2) the investigation or activity does not arise out of, and is not directly related to, (a) the receipt of Treatment; (b) a claim for public benefits related to Health Care; or (c) qualification for, or receipt of, public benefits or services in which the Individual’s health is integral to the claim.

7. Law enforcement purposes.

- a. General rule. If state law requires Covered Entities to report certain statistics (e.g., gunshot wounds, stab wounds, burns, etc.) to law enforcement officials, such Disclosures do not require a verbal agreement or authorization. Disclosures may also be made pursuant to (i) a court order; (ii) a subpoena or summons issued by a judicial officer; (iii) a state or federal grand jury subpoena; (iv) administrative subpoenas or summons; (v) civil investigative demands; or (vi) other similar process allowed by law. All such requests for Disclosures for law enforcement purposes must satisfy the following requirements:
- (1) be specific and limited in scope to the extent reasonably practical in light of the purpose for which the PHI is sought;
  - (2) be relevant and material to a legitimate law enforcement inquiry; and

(3) be incapable of using “de-identified” PHI to satisfy the purpose of the requested Disclosure.

b. Limited identifying information. Covered Entities may also Disclose “limited identifying information” for purposes of identifying suspects, witnesses, missing persons, etc., when law enforcement officials are seeking to identify and/or locate a person. Covered Entities cannot, however, initiate the Disclosure. The request can be made verbally or in writing by a law enforcement official or his or her representative. “Limited identifying information” consists of the following: (i) name, (ii) address, (iii) social security number, (iv) date of birth, (v) type of injury, (vi) ABO blood type, (vii) Rh factor, (viii) date and time of death, (ix) date and time of treatment, and (x) distinguishing physical characteristics of the person. Specifically *excluded* from the list of “limited identifying information” are DNA records, dental records, and bodily fluids other than blood.

8. Crime victims.

a. General rule. Unless the requested Disclosure is permitted pursuant to the victims of abuse, neglect, or domestic violence rule discussed above, a Health-Care Provider must obtain the Individual’s verbal agreement before Disclosing PHI to a law enforcement official. A Health-Care Provider cannot initiate the Disclosure; it must be in response to a request from a law enforcement official.

b. Incapacitated Individuals or emergencies. If an Individual is unable to give a verbal agreement due to incapacity or if there is an emergency situation, a Health-Care Provider *may* disclose PHI for purposes of this rule if:

(1) the law enforcement official represents that PHI is needed to determine whether a violation of law by a person other than the victim has occurred and the PHI will not be used against the victim;

(2) the law enforcement official represents that the law enforcement activity will be materially and adversely affected by waiting for the Individual’s verbal agreement; and

(3) the Health-Care Provider in his or her professional judgment believes that it would be in the Individual’s best interest to make the Disclosure.

- c. Deaths. Health-Care Providers can also inform law enforcement officials of a death of an individual if they have a suspicion that such death may have resulted from criminal conduct.
  - d. Evidence of crimes. Health-Care Providers may also Disclose PHI to law enforcement officials if they believe in good faith that it constitutes evidence of a crime committed on their premises.
  - e. Offsite emergency care. A Health-Care Provider providing emergency Treatment in response to a medical emergency (other than an emergency on the premises of a Covered Entity) may Disclose PHI to a law enforcement official if such Disclosure appears necessary to alert the law enforcement official to any of the following, unless the Health-Care Provider believes the medical emergency is the result of abuse, neglect, or domestic violence (in which case the rule applicable to such situations discussed above applies):
    - (1) the commission and nature of a crime;
    - (2) the location of such crime or victims of such crime; or
    - (3) the identity, description, or location of the perpetrator of such crime.
  - f. Objects that are not PHI. Weapons, clothing, knives, guns, etc., are not considered PHI. Communications made in conjunction with the receipt or maintenance of such items, however, are *possibly* PHI.
9. Coroners, medical examiners (“MEs”), and funeral directors. Covered Entities can Disclose PHI to coroners, medical examiners, and funeral directors. In addition, they can include identifying information about other persons contained in the deceased Individual’s medical record.
  10. Organ procurement/donation. Covered Entities may Disclose PHI to procurement organizations or other entities engaged in the procurement, banking, or transplant of cadaveric organs, eyes, or tissue. This rule is intended to address situations in which the Individual has not previously indicated a preference to donate.
  11. Aversion of serious threats to the health or safety of a person or the public. Covered Entities may Use or Disclose PHI if they have a reasonable belief that the Use or Disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. The Use or Disclosure must occur in an emergency situation and be to persons reasonably able to prevent or lessen the threat.

12. Military personnel. Covered Entities providing Treatment to U.S. Armed Forces personnel are authorized to Disclose PHI for activities deemed necessary by appropriate military command authorities to ensure proper execution of military missions. Foreign military personnel are completely exempt from protection by the Privacy Regulations.
13. Inmates. No verbal agreement or authorization is required for the Use or Disclosure of PHI for an Individual who is part of a criminal justice system or in lawful custody (i.e., not just detained). After the Inmate is released, however, the normal rules of the Privacy Regulations are applicable to the Individual.
14. Workers' Compensation. Covered Entities may Disclose PHI to (i) a person or entity responsible for the Payment of benefits on behalf of an Individual for a claim covered by the state's workers' compensation law or (ii) the state's workers' compensation agency responsible for administering claims. The amount of PHI Disclosed, however, must satisfy the "minimum necessary" requirement (see Section V.D, below).

D. "Minimum necessary" requirement.

1. General rule. For all Uses, as well as many Disclosures and requests for Disclosures from other Covered Entities, a Covered Entity must implement policies and procedures that ensure that only the "minimum necessary" PHI is Used or Disclosed. "Minimum necessary" refers to the most limited amount of PHI that can be Used or Disclosed by the Covered Entity that still enables the purpose of the Use or Disclosure to be accomplished. Covered Entities must, in advance, establish and follow explicit policies and procedures that satisfy the following requirements:
  - a. identifies the persons or classes of persons who need access to PHI and the specific categories of PHI to which they are thereby authorized to have access in order to carry out their job-related duties;
  - b. identifies the specific conditions and time-frames under which such persons need access to each specific category of PHI;
  - c. establishes parameters to ensure that only the "minimum necessary" PHI is Used or Disclosed in response to requests that are made on a routine or recurring basis; and
  - d. establishes parameters for Disclosures to Business Associates and for other non-routine Disclosures.

2. Exceptions. The following Disclosures do not have to satisfy the “minimum necessary” requirement:
    - a. to a Health-Care Provider for Treatment of the Individual;
    - b. to the Individual himself or herself;
    - c. pursuant to an authorization by the Individual; or
    - d. pursuant to a request by HHS.
  3. Disclosures of entire medical records. Disclosure of entire medical records should not be made except pursuant to policies that specifically describe and justify when and why the entire medical record is needed.
  4. Requests from other Covered Entities. A Covered Entity should establish policies and procedures for responding to requests for PHI from other Covered Entities received on a routine basis. For non-routine requests, the Covered Entity must make individual decisions on a case-by-case basis. The Covered Entity, however, may reasonably rely on the other Covered Entity’s claim that its request is for the “minimum necessary” PHI to accomplish the purpose of the request.
  5. Research. For Research (see Section V.G, below), a Covered Entity can reasonably rely on documentation from the IRB or the Privacy Board that describes the PHI needed for the Research and asserts that the PHI requested is necessary to either prepare a Research protocol or for Research on decedents. The request must state with sufficient specificity that the PHI is necessary for Research.
- E. When a Covered Entity is required to Disclose PHI. The only three (3) instances in which a Covered Entity is *required* to Disclose PHI is if (i) the Individual requests such information about himself or herself; (ii) HHS compels such a Disclosure for compliance or enforcement purposes; or (iii) the Disclosure is otherwise required by law.
1. Disclosures required by law. Covered Entities are required to comply with laws regarding the Use or Disclosure of PHI. Covered Entities, however, must verify the identity/authority of persons who are seeking purportedly legally required Disclosures of PHI. The “minimum necessary” requirement (see Section V.D, above) does *not* apply in these situations, but the Disclosure of PHI must nonetheless be limited in scope to the information necessary to meet the requirements of the law that compels the Disclosure. A Covered Entity will not be sanctioned for violating the Privacy Regulations if the Disclosure was improper but was made in good faith by the Covered Entity. Even in circumstances in

which a Disclosure is required by law, a Covered Entity can still challenge the request.

2. Disclosures by Whistleblowers and Workforce member crime victims.

- a. Whistleblowers. Covered Entities are *not* in violation of the Privacy Regulations if a Disclosure of PHI is made in good faith by a member of its Workforce or a member of one of its Business Associates, provided that the Disclosure is to one of the following: (i) a Health Oversight Agency or public authority that is authorized by law to investigate or oversee the conduct of the Covered Entity; (ii) an appropriate health care accreditation organization (e.g., JCAHO); or (iii) an attorney for purposes of determining the Disclosing whistleblower's options. This rule only applies to whistleblower actions against a Covered Entity, not actions to expose malfeasant conduct of another person.
- b. Crime victims. As for a Workforce member who is a victim of a crime, the member may Disclose the location and other identifying information (to the extent it is not PHI) about an alleged perpetrator.

F. Affiliated Entities and Business Associates. Affiliated Entities may use a single, shared notice of privacy practices form. Business Associates may only Use PHI as permitted by their contracts with the Covered Entity.

G. Research.

1. General rule. A Covered Entity that desires to use or disclose PHI for Research purposes may *not* do so without a written Authorization from the Individual. This Authorization for Research may be: (i) contained in the same document as a consent to participate in the Research; or (ii) a separate written Authorization as discussed below. In any case, the Authorization must satisfy the general requirements applicable to Authorizations (see Section V.A, above) and, in addition, specify the Covered Entity's ability to condition Research-related Treatment on whether the Individual signs the Authorization.
2. Exceptions: Waivers and Alterations of Authorization. A Covered Entity may Use or Disclose PHI for Research purposes without obtaining an Authorization from the Individual *only if* the following criteria are satisfied:
  - a. for a waiver of Authorization (or alteration to the Authorization);
    - (1) the waiver or alteration is approved by an appropriately composed IRB;

- (2) the date of approval of such waiver and the signature of the IRB chair (or IRB designee) is on such approval; and
  - (3) documentation from the IRB is included that evidences the IRB's determination that:
    - (i) the Research could not practicably be conducted without the waiver or alteration;
    - (ii) the Research could not practicably be conducted without access to the PHI;
    - (iii) the Use or Disclosure of PHI involves no more than minimal risk to the privacy of the Individual, based upon, at least, the presence of the following elements:
      - (A) an adequate plan to protect any Identifiers from being improperly Used or Disclosed is in place;
      - (B) an adequate plan to destroy all Identifiers at the earliest opportunity, consistent with the conduct of Research is in place, unless there is a health or Research justification for retaining the Identifiers, or such retention is otherwise required by law; and
      - (C) adequate written assurances are obtained from any third party receiving such PHI that such third party will not re-Use or further Disclose the PHI, except as required by law, to oversee the Research projects, or for other Research for which the Use or Disclosure of the PHI would be permissible under the Privacy Regulations.
- b. for reviews preparatory to Research, the researcher represents that (a) the Use or Disclosure is solely for the purpose of preparing a Research protocol or similar preparatory purposes; (b) no PHI will be removed from the Covered Entity; and (c) the PHI is necessary for the Research; and
  - c. for Research involving a deceased Individual's PHI, the researcher (a) represents that the Use or Disclosure is sought solely for Research involving the deceased Individual's PHI; (b) provides

documentation on the death of the Individual, upon request; and (c) represents that the PHI is necessary for the Research.

3. Documentation of the IRB's or privacy board's approval of a waiver or alteration of authorization. If the IRB or privacy board waives or alters the authorization, this decision must be documented and include the following information:
  - a. the identity of the IRB or privacy board and the date of the action;
  - b. statements that the decision satisfies the following criteria: (a) the Use or Disclosure of PHI involves minimal risk to Individuals; (b) the decision will not adversely affect the privacy rights and welfare of Individuals; (c) the Research could not practically be conducted without the waiver or alteration; (d) the Research could not practically be conducted without the PHI; (e) the privacy risks are reasonable in relation to the anticipated benefits of the Research; (f) an adequate plan exists to protect Individual Identifiers from improper Use or Disclosure; (g) an adequate plan exists to destroy the Individual Identifiers at the earliest opportunity; and (h) adequate written assurances ensure that the PHI will not be reused or Disclosed to any other person 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;
  - c. a brief description of the PHI for which Use or access has been deemed necessary by the researcher;
  - d. a statement that the decision to waive or alter the authorization was reviewed and approved under normal or expedited review procedures; and
  - e. the signature of the chair of the IRB or privacy board or other member designated by such chair.

## **VI. Business Associates.**

- A. Existence of a Business Associate relationship. In general, a Business Associate relationship arises only if (i) a Covered Entity is Disclosing PHI to a person or entity that will Use the PHI on behalf of the Covered Entity, (ii) another person or entity will be creating or obtaining PHI on behalf of the Covered Entity, or (iii) another person or entity is providing the specified services to the Covered Entity and the provision of these services involves the Covered Entity Disclosing PHI to that person or entity. A Business Associate relationship does *not* arise if the person or entity in question is (a) a member of the Covered Entity's Workforce or (b) part of an organized health care arrangement in which the Covered Entity participates and it is for the purpose of enabling the organized health care

arrangement to perform its functions or services on behalf of the Covered Entity. Affiliated Entities are considered a single Covered Entity and, therefore, are not one another's Business Associate. For instance, BJC HealthCare and all of its member entities are considered a single Covered Entity.

- B. Business Associate contracts. A Covered Entity must obtain specific satisfactory assurances, in the form of a written contract, from each of its Business Associates that they will adequately protect PHI.
1. When a Business Associate contract is *not* necessary. A Covered Entity is not required to obtain from a Business Associate the contract described above if the Business Associate is a Health-Care Provider and the Disclosure of PHI concerns Treatment of the Individual. In addition, certain Disclosures by a group health plan, health insurance issuer, or HMO, as well as certain Uses and Disclosures by, or to, a government-sponsored Health Plan (e.g., Medicare), do not require a Business Associate contract.
  2. Required elements of Business Associate contracts. The Business Associate contract must:
    - a. be in writing;
    - b. describe the permitted Uses and Disclosures of PHI by the Business Associate;
    - c. provide that the Business Associate will:
      - (1) not Use or further Disclose PHI other than as permitted by the Business Associate contract or as required by law;
      - (2) use appropriate safeguards to prevent the Use or Disclosure of PHI;
      - (3) report to the Covered Entity any Use or Disclosure of PHI not provided for by its contract of which it becomes aware;
      - (4) ensure that any agents, including subcontractors, to whom the Business Associate provides PHI, agree to the same restrictions and conditions as contained in the Business Associate contract;
      - (5) make PHI available for Individuals to access, inspect, and copy;

- (6) make PHI available to Individuals for amendment and incorporate into the PHI any amendments requested by an Individual;
  - (7) make available to the Covered Entity the information required to provide an accounting of Disclosures to Individuals;
  - (8) make its internal practices, books, and records available to HHS to enable it to determine the Covered Entity's compliance with the Privacy Regulations; and
  - (9) upon the termination of the Business Associate contract, if feasible, return to the Covered Entity all PHI or destroy it and retain no copies, or, if such return or destruction is not feasible, extend the protections of the Business Associate contract to the PHI and limit further Uses and Disclosures to those purposes that make the return or destruction of the PHI infeasible; and
- d. authorize termination of the Business Associate contract by the Covered Entity if the Business Associate violates a material term of the contract.
3. Violations of the general rule governing Disclosures of PHI to Business Associates. The following constitute violations of the Privacy Regulations, *despite the existence of a written Business Associate contract*: (i) a Covered Entity violates the satisfactory assurances that it provided to another Covered Entity as a Business Associate of that Covered Entity; or (ii) a Covered Entity knew (or should have known) of a pattern of activity or practice of its Business Associate that constituted a material breach or violation of the Business Associate contract, unless the Covered Entity took reasonable steps to cure the breach or end the violation, and, if such steps were unsuccessful, the Covered Entity either terminated the contract or arrangement, if feasible, or if termination was not feasible, the Covered Entity reported the problem to HHS.

## **VII. Individuals' Rights Under the Privacy Regulations.**

- A. Individuals have five enumerated rights. The Privacy Regulations establish five (5) rights for Individuals with regard to their PHI. These rights focus generally on an Individual's right to regulate the Use and Disclosure of his or her PHI and consist of the following:
- 1. the right to notice of privacy practices by the Covered Entity;

2. the right to request privacy protections for PHI, including the right to restrict Uses or Disclosures and the right to designate methods for confidential communications;
3. the right to access his or her PHI;
4. the right to request an amendment of his or her PHI; and
5. the right to an accounting of the Disclosures of PHI by the Covered Entity.

B. The right to notice of the Covered Entity's privacy practices for PHI. Most Covered Entities are required to provide a notice of their privacy practices to Individuals. Covered Entities may not Use or Disclose PHI in a manner that is inconsistent with its notice and must obtain a written acknowledgment from Individuals demonstrating an Individual's receipt of the Covered Entity's notice of privacy practices.

If a written acknowledgment is not obtained from an Individual, a Covered Entity must document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained. If a Covered Entity did not obtain the acknowledgment due to an emergency treatment situation, the Covered Entity remains obligated to obtain the written acknowledgment as soon as is practicable following the emergency treatment. A Covered Entity must retain a copy of all the notices issued and the written acknowledgments for each Individual receiving a notice or the documentation of its good faith efforts to obtain such Individual's acknowledgment.

1. Required elements of an adequate notice. All notices of a Covered Entity's privacy practices must satisfy the following nine (9) requirements:

- a. Be written in plain language.
- b. Privacy header. In a header or other prominently displayed location, contain the following statement:

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

- c. Descriptions of PHI Uses and Disclosures. Contain several descriptions of sufficient detail concerning the required and permitted Uses and Disclosures of the PHI. Specifically, the notice must contain:

- (1) a description, together with at least one (1) example, of the types of Uses and Disclosures permitted by the Privacy Regulations for each of the following purposes: Treatment, Payment, and Health Care Operations;
  - (2) a description of each of the other purposes that the Covered Entity is permitted or required to Use or Disclose PHI without the Individual's authorization;
  - (3) a description of any more stringent state law as to any particular Use or Disclosure of PHI; and
  - (4) a statement that any other Uses or Disclosures will be made only with the Individual's written authorization and that the Individual may revoke such authorization.
- d. Separate statement for certain Uses or Disclosures. Contain a statement that the Individual may be contacted either to provide, among other things, appointment reminders or other health-related benefits, or for Fund-raising purposes, if the Covered Entity engages in those activities.
  - e. Description of an Individual's rights. Contain a statement of an Individual's five (5) rights with respect to PHI and a brief description of how an Individual may exercise such rights.
  - f. Description of the Covered Entity's duties. Contain a statement explaining the Covered Entity's legal duties with respect to protecting and maintaining the privacy of PHI.
  - g. Inform Individuals of the ability to file complaints. Contain a statement informing Individuals of their right to file a complaint with the Covered Entity and/or HHS if they believe that a violation of their privacy rights has occurred. In addition, the notice must include a description of the process to file a complaint and inform Individuals that they will not be retaliated against for filing a complaint.
  - h. Providing a contact. Identify the name (or title) and telephone number of the person to contact for further information.
  - i. Effective date. Contain an effective date for the notice that may not be earlier than its date of publication.
2. Optional elements of notice. In addition to the required elements of a notice, a Covered Entity may opt to further limit the Uses or Disclosures

of PHI, but only to the extent that any additional limitations do not affect a required or otherwise permitted Use or Disclosure.

3. Revisions to the notice. The Covered Entity must promptly modify and distribute a revised notice whenever there is a material change to the Uses or Disclosures, the Individual's rights, the Covered Entity's legal duties, or other privacy practices concerning PHI.

4. When and how the notice must be provided. Generally, Covered Entities must provide the required notice on request to any Individual or other person.

a. Health-Care Providers. For Health-Care Providers who have a Direct Treatment Relationship with an Individual, the notice must (a) be provided no later than the date of the first service delivery to the Individual; (b) if the Health-Care Provider maintains a physical service delivery site (e.g., a hospital office or other location where services are provided), be posted in a clear and prominent location where it can be reasonably expected to enable Individuals seeking services to read it and be made available to Individuals to take with them; and (c) be promptly distributed on or after revision dates, including updates to any posted notices.

b. Organized health care arrangements: joint notices. Covered Entities participating in organized health care arrangements may elect to issue a joint notice for the participating Covered Entities. If a joint notice will be issued, all the participating Covered Entities must agree to abide by the terms of the joint notice concerning PHI. Additionally, the joint notice must contain the required elements discussed above, with the exception that the statements in the notice may be altered as necessary to reflect the additional Covered Entities. The joint notice also must list the applicable Covered Entities and service delivery sites to which the joint notice applies. Finally, the joint notice must state that the participating Covered Entities will share PHI with each other as necessary to carry out TPO relating to the organized delivery arrangement.

C. The right to request privacy protections, including the right to restrict Uses or Disclosures and the right to designate methods for confidential communications.

1. General rule. A Covered Entity must permit an Individual to request that the Covered Entity restrict the Uses or Disclosures of PHI for TPO, including persons involved in such care, and to accommodate reasonable requests concerning how an Individual receives confidential communications concerning PHI.

2. The right to request restrictions on the Uses or Disclosures of PHI.  
Covered Entities must permit Individuals to request certain restrictions on Uses and Disclosures affecting their PHI. The PHI subject to restrictions are divided into two (2) categories: (i) Uses and Disclosures of PHI to carry out TPO; and (ii) Disclosures to persons involved in the Individual's care. Covered Entities are *not* required to agree to any requested restrictions in either category. If, however, a Covered Entity agrees to any restrictions, it may not Use or Disclose PHI in violation of such restrictions (except in emergencies), and must document the restrictions.
  - a. Emergency exception. If the Use or Disclosure is for emergency Treatment and the restricted PHI is needed to provide emergency Treatment, the Covered Entity may Use or Disclose the PHI to provide the Treatment. If such PHI is Used or Disclosed incident to this exception, the Covered Entity must request that the receiving Health-Care Provider not further Use or Disclose the PHI.
  - b. Other exceptions. Notwithstanding any agreement for a restriction, the Covered Entity may Use or Disclose PHI permitted or required by (a) a request by the Individual; (b) the Covered Entity's Facility Directory (see Section V.B.2, above); or (c) law or for public health purposes.
  - c. Terminating a restriction. Covered Entities may terminate an agreement to restrict PHI if (a) the Individual agrees to or requests the termination in writing; (b) the Individual verbally agrees to the termination and the verbal agreement is documented by the Covered Entity; and (c) the Covered Entity informs the Individual of its decision to terminate the restriction. If the termination is at the request of the Covered Entity, it is only effective with regard to PHI created or received after it has informed the Individual of its decision to terminate the restriction.
3. The right to designate methods for confidential communications.  
Individuals may request alternative means of receiving PHI from Covered Entities. The standards governing a Covered Entity's response to a request varies according to the type of Covered Entity.
  - a. Health-Care Providers. A Health-Care Provider must permit Individuals to request that they receive communications of PHI from the Health-Care Provider by alternative means or at alternative locations. In addition, the Health-Care Provider must accommodate such requests if they are reasonable.

- b. Health Plans. As with Health-Care Providers, Health Plans must also permit and accommodate reasonable requests, but only if the Individual clearly asserts that the Disclosure of all or part of the PHI could endanger the Individual.
- c. Conditions on requests for confidential communications. Covered Entities may impose some limited conditions on requests for confidential communications, such as (a) requiring Individuals to submit written requests for alternate methods of confidential communications; (b) conditioning the reasonable accommodation on information concerning how Payment, if any, will be handled; or (c) requiring Individuals to specify an alternative address or other method of contact.

D. The right of access to PHI.

- 1. General rule. An Individual has a right to access and copy his or her PHI contained within a Designated Record Set. Covered Entities must define the Designated Record Sets that are subject to requests for access by Individuals and document the titles of persons or offices responsible for receiving and processing such requests.
- 2. Exceptions. Individuals do not have a general right of access to their PHI contained within a Designated Record Set if such PHI is:
  - a. maintained in Psychotherapy Notes;
  - b. compiled in reasonable anticipation of a civil, criminal, or administrative action or other proceeding; or
  - c. maintained for compliance with CLIA and is prohibited or exempt from Disclosure under that statute.
- 3. Denial of access. Individual requests for access to PHI may be denied by a Covered Entity on several grounds. Once a request is denied, an Individual, depending on the reason for the denial, may be entitled to a review of the denial by the Covered Entity.
  - a. Unreviewable grounds for denial of access to PHI. The following constitute circumstances in which a Covered Entity's decision to deny an Individual access to his or her PHI is *unreviewable*:
    - (1) the PHI consists of Psychotherapy Notes;
    - (2) the PHI is compiled in reasonable anticipation of a civil, criminal, or administrative action or other proceeding;

- (3) the PHI is maintained for compliance with CLIA and is prohibited or exempt from Disclosure under that statute;
- (4) the request is from an Inmate and the Covered Entity is a correctional institution or is rendering services under the direction of a correctional institution and the PHI would jeopardize the health or safety of other persons;
- (5) the PHI was created or obtained by a Health-Care Provider in the course of Research in which the Individual consented to the denial of access when consenting to participate in the Research and the Health-Care Provider informed the Individual that he or she would have access to the PHI upon completion of the Research;
- (6) the PHI is contained in records subject to HIPAA and that statute permits the denial of access; or
- (7) the PHI was obtained from someone other than a Health-Care Provider under a promise of confidentiality and the access would be reasonably likely to reveal that person as the source of the PHI (e.g., a former sex partner).

b. Reviewable grounds for denial of access to PHI. A denial of access is *reviewable* by a licensed health care professional if it is for any of the following reasons:

- (1) Access is reasonably likely to endanger the life or physical safety of the Individual or another person as determined by a licensed health care professional using professional judgment;
- (2) The PHI references another person (excluding other licensed health care professionals) and the access requested is reasonably likely to cause substantial harm to such other person as determined by a licensed health care professional using professional judgment; or
- (3) The request is made by the Individual's personal representative and the access to the personal representative is reasonably likely to cause substantial harm to the Individual or another person as determined by a licensed health care professional using professional judgment.

c. Process to deny access and provide for review for reviewable denials. Regardless of whether a denial of access is reviewable,

the Covered Entity must comply with the process for denying access.

- (1) Process for denying access. If the Covered Entity denies access to PHI (either in whole or in part), it must (a) to the extent possible, provide access to non-excluded PHI and (b) provide a timely, written denial to the Individual that is written in plain language and explains (i) the ground(s) for the denial, (ii) the review rights, if any, available to the Individual, including a description of how the Individual may initiate a review, and (iii) how the Individual may complain to the Covered Entity or HHS. This notice of denial must also contain the name or title and telephone number of the contact person or office at the Covered Entity. Additionally, if the Covered Entity does not maintain the requested PHI, it must inform the Individual where the PHI is located.
  - (2) Request for review of a denial. If access to the PHI is denied based upon reviewable grounds, as discussed above, and the Individual requests a review of such decision, the Covered Entity must promptly refer a request for review to a Designated L.P. The Designated L.P. must not be involved directly with the decision to deny access to PHI. After receiving a request for review of a denial, the Designated L.P. must determine, within a reasonable period of time, whether or not to deny the access requested based upon the reviewable grounds standards discussed above. The Covered Entity is bound by the determinations of the Designated L.P. and must promptly provide written notice of his or her determination with regard to an Individual's request and take the appropriate action, if any.
4. Form of the request. The Privacy Regulations do not mandate a specific form for requests to access PHI. Covered Entities may, however, require that requests for access to PHI be made in writing if they first inform Individuals that they are establishing such a requirement.
  5. Timeframes for Covered Entity responses to requests for access. In general, a Covered Entity must respond in writing to a request (i.e., grant or deny access) no later than thirty (30) days after receiving such a request. In addition, if the response is a grant of access, the Covered Entity must provide the appropriate access to the PHI within such timeframe. If the PHI is maintained in offsite storage or is not accessible to the Covered Entity onsite, the Covered Entity has an additional thirty (30) days to respond to the request (i.e., sixty (60) days total). Covered Entities may also obtain a one-time extension, of no more than thirty (30)

days, to respond to a request for access. To obtain such an extension, a Covered Entity must inform the requesting Individual, in writing, within thirty (30) days (or sixty (60) days for offsite storage) of its receipt of the request that there will be a delay in its response, including a statement of the reasons for the delay and the date by which the Covered Entity will have a response.

6. Provision of access. If the Covered Entity grants access to the PHI, it must (i) provide the access requested either through inspection, copying, or both and (ii) provide the PHI in the form requested, if readily producible in such form; if not, then in hard copy. Alternatively, a Covered Entity may produce summaries of the PHI requested in lieu of providing the PHI itself, provided that the Covered Entity first obtains the Individual's agreement to receive a summary and to pay for any fees related to the summary.
7. Fees. The Covered Entity may charge the Individual a reasonable cost-based fee for copying the PHI. The fee may only include the cost of copying (including labor and supply costs), postage, and the preparation of any summary (if agreed to by the Individual).

E. The right to request an amendment of PHI.

1. General rule. An Individual has the right to request that a Covered Entity amend his or her PHI that is contained in a Designated Record Set. A Covered Entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments and retain the documentation in accordance with the Privacy Regulations.
2. Procedures for requests. Covered Entities may require that requests for amendment be in writing and include a reason to support the amendment. Individuals must be informed of these requirements prior to their request for amendment. Covered Entities must grant, deny, or obtain an extension concerning a request for an amendment no later than sixty (60) days following receipt of a request. A Covered Entity may obtain a one-time extension of no more than thirty (30) days by providing a written statement to the Individual explaining the reasons for the delay and the date by which the Covered Entity will respond to the request.
3. Grants of requests for amendment.
  - a. Procedure. If a Covered Entity accepts a request for an amendment (in whole or in part), it must:
    - (1) make the appropriate amendment to the PHI by, at a minimum, identifying the PHI in the Designated Record Set that is affected by the amendment and appending or

otherwise linking the original PHI to the location of the amendment;

- (2) inform the Individual that it has accepted the request for amendment and obtain the Individual's identification of the other persons and entities that should receive a copy of the amendment and the Individual's agreement to have the Covered Entity provide a copy of the amendment to such other persons and entities; and
- (3) make reasonable efforts to inform and provide, within a reasonable time, the amendment to persons and entities identified by the Individual or that the Covered Entity knows have the relevant PHI and that could rely (or may have already relied) on such PHI.

b. Grants by another Covered Entity. Covered Entities must amend PHI in their possession to the extent that they receive notice from another Covered Entity that it granted an Individual's request for amendment affecting that PHI.

4. Denials of requests for an amendment.

a. Reasons. A Covered Entity may only deny a request for amendment of PHI if it determines that the relevant PHI:

- (1) was not created by the Covered Entity (unless the requestor believes that the originator is no longer available);
- (2) is not a part of a Designated Record Set;
- (3) is not available for access (see Section VII.D, above); or
- (4) is accurate and complete.

b. Procedures. If the Covered Entity denies (in whole or in part) the request for amendment, it must, in plain language, provide a timely written denial to the Individual that:

- (1) states which of the above reasons is the basis for the denial;
- (2) states the Individual's right to submit a written statement disagreeing with the denial and how to file the statement of disagreement with the Covered Entity;
- (3) contains a statement informing the Individual that if he or she chooses not to file a statement of disagreement, that he

or she may, alternatively, request that the Covered Entity include his or her request for amendment, as well as the denial of such amendment, with any future Disclosures of the PHI that was the subject of the request; and

(4) contains a description of the complaint process that the Individual may follow with HHS or the Covered Entity, including the name or title and telephone number of the contact person.

c. Statements of disagreement. A Covered Entity *must* accept any statement submitted by an Individual that disagrees with the denial of all or part of a requested amendment. The Covered Entity may, however, reasonably limit the length of the statement submitted. Additionally, the Covered Entity may prepare a rebuttal statement to any statement of disagreement submitted, in which case it must provide a copy of the rebuttal statement to the Individual.

d. Future Disclosures relating to denials. A Covered Entity must identify the PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the Individual's request for an amendment, the denial of the request, the statement of disagreement (if any), and the Covered Entity's rebuttal, (if any) (collectively, "denial materials"). If the Individual submitted a statement of disagreement, the Covered Entity must either include the denial materials or, at its election, an accurate summary of the denial materials, with any subsequent Disclosures of the PHI to which the disagreement relates. If the Individual did *not* submit a statement of disagreement and the Individual has requested the inclusion of the request and denial for amendment in any future Disclosures, the Covered Entity must either include the Individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent Disclosure.

F. The right to an accounting of Disclosures of PHI.

1. General rule. An Individual has the right to receive an accounting from a Covered Entity as to Disclosures that it has made of that Individual's PHI during the six (6) year period preceding the date that the Covered Entity receives the request. Individuals may also request an accounting for any period less than the six (6) year limit.

2. Exceptions. Exceptions to the general rule governing accounting of Disclosures include Disclosures that were made for any one of the following purposes:

- a. To carry out TPO;
  - b. To Individuals who have requested access to their PHI;
  - c. Incident to a Use or Disclosure otherwise permitted or required by the Privacy Regulations;
  - d. Pursuant to an Individual's authorization (see Section V.A, above);
  - e. For use in the Health-Care Provider's Facility Directory;
  - f. To persons involved in the Individual's care;
  - g. For national security or intelligence purposes;
  - h. To correctional institutions or law enforcement officials in accordance with the rules governing Inmates;
  - i. As part of a Limited Data Set; or
  - j. That occurred prior to April 14, 2003.
3. Procedures for responding to requests for an accounting. A Covered Entity must act on a request for an accounting no later than sixty (60) days following its receipt of a request by either providing the requested accounting or, if it is unable to provide the accounting within (60) days, informing the Individual that it will be exercising a one-time extension of no more than thirty (30) days in which to complete its response. In order to obtain an extension, the Covered Entity must provide the Individual with a written statement of the reasons for the delay and the date by which it will provide the accounting.
4. Fees. Covered Entities must provide the first accounting to an Individual in any twelve (12) month period free of charge. For each subsequent request by the same Individual within the same twelve (12) month period, the Covered Entity may impose a reasonable cost-based fee. In imposing any fee for an accounting, however, the Covered Entity must first inform the Individual of the fee and provide the Individual with an opportunity to withdraw or modify his or her request in order to avoid or reduce the fee.
5. Suspension of an Individual's right to an accounting. A Covered Entity *must* temporarily suspend an Individual's accounting right for a specified time if a Health Oversight Agency or law enforcement official specifies, *in writing*, (i) that the accounting would be reasonably likely to impede the Health Oversight Agency's or law enforcement official's activities and (ii) the time period for the required suspension. Although written suspensions are preferred, a Health Oversight Agency or law enforcement

official may make *verbal* requests for suspension, in which case the Covered Entity must (a) document the name of the Health Oversight Agency or law enforcement official and the statement requesting suspension, (b) temporarily suspend the accounting, and (c) limit the suspension to no longer than thirty (30) days unless it receives a written statement from the Health Oversight Agency or law enforcement official.

6. Content of the accounting.

a. General requirements. In responding to a request for an accounting, the Covered Entity must provide a written accounting that includes:

- (1) all the Disclosures of PHI, including Disclosures to, or by, Business Associates, occurring before the request date and within the requested period, except for PHI excluded from Disclosure;
- (2) for each Disclosure, the date of the Disclosure, the name of the person or entity receiving the PHI, and, if known, the address of the person or entity;
- (3) for each Disclosure, a brief description of the PHI Disclosed; and
- (4) for each Disclosure, a brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure, or, in lieu of a statement, a copy of the written request for Disclosure.

b. Multiple Disclosures. If the Covered Entity made multiple Disclosures during the requested accounting period of the PHI to the *same* person or entity for a single purpose or pursuant to a single authorization, the accounting may, with respect to such multiple Disclosures, provide the information required above for the first Disclosure and a listing of the frequency, periodicity, or number of the Disclosures during the period and the date of the last Disclosure.

c. Research Disclosures. If, during the period covered by the requested accounting, the Covered Entity made Disclosures of PHI for a particular Research purpose in accordance with the Privacy Regulations for more than fifty (50) Individuals, the accounting may, with respect to such Disclosures, provide:

- (1) the name of the protocol or other Research activity;

- (2) a description, in plain language, of the Research protocol or other Research activity, including the purpose of the Research and the criteria for selecting particular records;
- (3) a brief description of the type of PHI Disclosed;
- (4) the date or period of time during which such Disclosures occurred or may have occurred, including the date of the last Disclosure;
- (5) the name, address, and telephone number of the entity that sponsored the Research and of the researcher receiving the PHI; and
- (6) a statement that the PHI of the Individual may or may not have been Disclosed for a particular protocol or other Research activity.

If a Covered Entity provides an accounting for Research Disclosures in the above manner and if it is reasonably likely that the PHI was Disclosed for such Research protocol, the Covered Entity must, upon request, assist the Individual in contacting the sponsoring entity and researcher.

## **VIII. Marketing and Fund-raising Activities.**

### **A. Marketing.**

1. What constitutes Marketing. As noted in Section II, above, “Marketing” is generally (and broadly) defined as a communication about a product or service that encourages recipients of the communication to purchase or to use the product or service. Additionally, Marketing also includes an arrangement between a Covered Entity and a third party whereby the Covered Entity Discloses PHI, in exchange for remuneration, for the third party to market its own products or services.
2. Communications that are *not* considered Marketing. The following, however, are exceptions to the definition of Marketing: (i) a communication made to describe a health-related product or service (or Payment for such product or service) that is provided by a Covered Entity or included in a plan of benefits, including; (a) entities participating in a Health Plan network; (b) replacement of, or enhancements to, a Health Plan; and (c) health-related products or services available only to a Health Plan enrollee that add value to, but are not a part of, a plan of benefits; or (ii) a communication made for Treatment of the Individual; or (iii) a communication made for case management or care coordination for that

Individual, or to direct or recommend alternative treatments, therapies, Health-Care Providers, or settings of care.

3. Uses and Disclosures of PHI for Marketing purposes.

- a. General rule. A Covered Entity may not Use or Disclose PHI for Marketing purposes without an authorization (see Section V.B, above) from the Individual. If the Marketing communication involves direct or indirect remuneration to the Covered Entity from a third party, the authorization must state that such remuneration is involved.
- b. Exceptions: The following Marketing communications (including Uses or Disclosures) may be made without prior authorization from the Individual: (i) a communication that occurs in a face-to-face encounter between the Covered Entity and the Individual; or (ii) a communication that concerns a promotional gift of nominal value.

B. Fund-raising.

1. Uses and Disclosures of PHI for Fund-raising purposes.

- a. General Rule: A Covered Entity may *not* Use or Disclose PHI for Fund-raising purposes without an authorization from the Individual (see Section V.B, above).
- b. Conditional Exceptions. A Covered Entity *may*, without obtaining an authorization from the Individual, (i) Use PHI that consists of demographic data relating to the Individual or the dates upon which Health Care was provided to the Individual or (ii) Disclose such information to a Business Associate or institutionally-related foundation, provided that the Covered Entity satisfies the following conditions:
  - (1) includes within its notice of privacy practices (see Section VII.B, above) a statement that the Covered Entity may contact the Individual to raise funds for the Covered Entity;
  - (2) includes with any Fund-raising materials it distributes a description of how the Individual can opt out of receiving any further Fund-raising communications; and
  - (3) makes reasonable efforts to ensure that Individuals who decide to opt out of receiving such future Fund-raising communications are indeed not sent such communications.

## **IX. Administrative Requirements.**

In addition to all of the other standards and rules, the Privacy Regulations impose upon Covered Entities seven (7) “administrative requirements,” consisting of the following:

- A. Privacy personnel. Covered Entities must appoint a “privacy official” and a “contact person” (who can be the same person), responsible for overseeing the Covered Entity’s policies, requirements, and compliance with the Privacy Regulations.
- B. Privacy policies and procedures. Covered Entities must implement written policies and procedures regarding how they will comply with the Privacy Regulations.
- C. Privacy training. All current employees of the Covered Entity must receive privacy education and training by April 2003. New employees must be trained soon after their date of hire.
- D. Privacy safeguards. Covered Entities must establish administrative, technical, and physical safeguards to protect the privacy of PHI.
- E. Privacy complaints. Covered Entities must establish processes to address Individuals’ complaints about their privacy procedures and to respond to alleged violations of the Privacy Regulations.
- F. Privacy sanctions and mitigation. Covered Entities must establish sanctions to discipline employees for violations of the Privacy Regulations. Covered Entities also have a duty to investigate any harmful effects of a violation.
- G. No intimidation or retaliation. Covered Entities cannot intimidate or retaliate against anyone who (i) participates in a process prescribed by the Privacy Regulations, (ii) files a complaint, alleging a violation of the Privacy Regulations, or (iii) opposes a practice that the person in good faith believes violates the Privacy Regulations.