The Health Insurance Portability and Accountability Act (HIPAA)

Guide to the HIPAA Privacy Rule

State of Ohio

HIPAA Statewide Project Privacy Workgroup

Revised per The HITECH Act

June 2012

Privacy Workgroup Members

The Privacy Rule Summary was developed by staff from the following state agencies in April 2002. A subsequent working group updated the Summary in 2012 per The HITECH Act.

2002 Workgroup

Ohio Department of Aging
Carla Dowling Fitzpatrick
Ohio Department of Alcohol and Drug Addiction Services
Jodi Locker
Sara Vollmer
The Attorney General's Office
Jordan Finegold, co-chair
Jim Evans
Ohio Department of Health
Socrates Tuch
Ohio Department of Job and Family Services
Joe Silver, co-chair
Dale Lehmann
Ohio Department of Mental Health
Janice Franke
Ohio Department of Mental Retardation and Developmental Disabilities
Marie Charvat
Ohio Department of Rehabilitation and Corrections
Katheryn Ehrle
Greg Trout
Ohio Veterans Home
Greg Kowalski
Bureau of Workers' Compensation
Pete Mihaly
Dora West
Ohio Department of Youth Services
Lew George

2012 Workgroup

Ohio Department of Administrative Services
Eric Harrell
Ohio Department of Aging
Stephanie Loucka
Ohio Department of Alcohol and Drug Addiction Services
James Lapczynski
The Attorney General's Office
Kathleen Madden
Ohio Department of Developmental Disabilities
Bradley Singer
Ohio Department of Health
Socrates Tuch
Ohio Department of Job and Family Services
Rick Copley, co-chair
Ohio Department of Mental Health
Geoff Callander
Office of Information Security & Privacy
Daren Arnold, co-chair
Kevin Brown
Robin Powell
Bureau of Workers' Compensation
Pete Mihaly

6/1/2012

TABLE OF CONTENTS

Contents

This document was developed to assist the state agencies of Ohio in understanding the obligations imposed by the Health Insurance Portability and Accountability Act (HIPAA). The State of Ohio provides no guarantee of accuracy or warranties of any kind. Utilization of this information is at the sole risk of the user. As with any matter of law, independent legal counsel should be consulted regarding compliance with the requirements of the HIPAA.

GUIDE TO HIPAA PRIVACY REGULATIONS

[45 CFR Parts 160 and 164]

A. DEFINITIONS [see 160.103, 160.202, 160.302, 164.501 for other definitions]:

1. Covered Entity (CE) means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction. *160.103*
   - a. Health plan means an individual plan or group plan that provides, or pays the cost of, medical care. [NOTE: includes the Medicaid and Medicare programs]
   - b. Health care clearinghouse means an entity that processes health information received in a nonstandard format into a standard format, or processes health information received in a standard format into a nonstandard format for another entity.
   - c. Health care provider means a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
2. Protected Health Information (PHI) means individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual. PHI excludes: *160.103*
   - a. individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (20 U.S.C. 1232g);
   - b. records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and;
   - c. employment records held by a CE in its role as employer.
3. Individually Identifiable Health Information is information that is a subset of health information, including demographic information collected from an individual, and: *164.103*
   - a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
   - b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
4. Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an *164.502(g)*

adult or an emancipated minor, or the parent, guardian, or other person acting in loco parentis who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or other person acting in loco parentis has assented to an agreement of confidentiality between the provider and the minor.

5. Treatment, Payment and Health Care Operations (TPO) includes all of the following: *164.501*

   a. Treatment means the provision, coordination or management of health care and related services, consultation between providers relating to an individual or referral of an individual to another provider for health care.

   b. Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.

   c. Health care operations includes functions such as: quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

6. Covered Functions means those functions of a CE, the performance of which make the entity a health plan, a health care clearinghouse or a health care provider. *164.501*

7. Hybrid Entity means a single legal entity that is a CE whose business activities include both covered and non-covered functions and that designates health care components in accordance with 164.504(c)(3)(iii) [¶ J. .3. .c. .iiiJ.3.c.iii]. *164.103*

8. Designated Record Set means a group of records maintained by or for a CE that is: the medical and billing records relating to an individual maintained by or for a health care provider; the enrollment, payment, claims adjudication and case or medical management systems maintained by or for a health plan; or used, in whole or part, by of for a CE to make decisions about individuals. *164.501*

9. Business Associate (BA) means a person or entity who, on behalf of the CE, and other than in the capacity of a workforce member: performs or assists in the performance of a function or activity that involves the use or disclosure of PHI; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. *160.103*

10. Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a CE, is under the direct control of such entity, whether or not they are paid by the entity. *160.103*

11. Health Oversight Agency means a governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is authorized by law to oversee the public or private health care system or government programs in which health *164.501*

information is necessary to determine eligibility or compliance, or to enforce civil rights for which health information is relevant.

12. Public Health Authority means a governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate. *164.501*

13. Indirect Treatment Relationship means a relationship between an individual and a health care provider in which the health care provider delivers health care to the individual based on the orders of another health care provider and the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual. *164.501*

14. Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. *164.501*

15. Health Care Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions: *164.501*

a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

c. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) [¶ C.6] are met, if applicable;

d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

e. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

f. Business management and general administrative activities of the entity, including, but not limited to: management activities relating to implementation of and compliance

with the requirements of this subchapter; customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; resolution of internal grievances; the sale, transfer, merger, or consolidation of all or part of the CE with another CE, or an entity that following such activity will become a CE and due diligence related to such activity; and consistent with the applicable requirements of § 164.514 [¶ C.10], creating de-identified health information, or a limited data set, and fundraising for the benefit of the covered entity.

16. Law Enforcement Official means a public employee from any branch of government who is empowered by law to investigate a potential violation of the law or to prosecute, or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. *164.103*

B. GENERAL RULES:

1. HIPAA privacy regulations preempt state law except where: *160.201-160.205*
   a. State law is determined by the Secretary of HHS to be necessary to prevent fraud and abuse related to the provision of or payment for health care, to ensure appropriate regulation of insurance and health plans, for state reporting on health care and delivery systems, or to serve a compelling need relating to public health, safety or welfare that outweighs the intrusion into privacy;
   b. State law has as its principal purpose the regulation of controlled substances;
   c. State law relates to privacy of individually identifiable health information and is more stringent than the regulations - i.e. state law meets one or more of the following criteria: prohibits or restricts a use/disclosure that would be permitted under the regulations, except where the disclosure required by the Secretary of HHS for determining a CE's compliance with the regulations, or where disclosure is to the individual who is the subject of the health information; allows the individual greater rights to access or amend his/her records; requires more information be provided to the individual about the use/disclosure of his/her records; narrows the scope or duration of, increases the privacy protections afforded by, or reduces the coercive effect of the circumstances surrounding the consent or authorization; requires more record keeping relating to uses/disclosures, or; otherwise provides greater privacy protections;
   d. State law provides for reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention, or;
   e. State law requires a health plan to report or provide access to information for management, financial, programmatic or licensure or certification audit.
2. Except as permitted or required under the privacy regulations, CEs may not use or disclose PHI without authorization. CE generally is required to allow individual access to his/her PHI, and to permit Secretary of HHS access to PHI for compliance/enforcement purposes. *164.502*
   a. Authorization: Allows use/disclosure of PHI for purposes beyond TPO; written in specific terms; must specify termination date/event/condition [¶ G].
   b. Exceptions: Regulations provide exceptions for such uses/disclosures as public health, oversight, law enforcement, legal process, safety, and research activities, etc. [¶ I]

3. CE must make reasonable efforts to provide or request only the minimum PHI necessary to accomplish the intended purpose of the use, disclosure or request. *164.502(b)*
4. Protection for PHI of deceased persons is the same as if still living. *164.502(f)*
5. CE is required to provide individuals with a Notice of Privacy Practices/Privacy Notice that gives sufficient notice of the uses/disclosures that CE may make of PHI, and of the individual's rights and the CE's duties relating to PHI. Inmates and correctional facilities are exempted from this right/obligation. *164.520*
6. CE is required to account to individual for most uses/disclosures of PHI made over a period of up to six years. *164.528*
7. Regulations impose administrative requirements upon CE, including development of policies, training of workforce, and documentation. *164.530*

C. USES AND DISCLOSURES:

1. Permitted Uses and Disclosures: CE is permitted to use/disclose PHI: *164.502(a)(1)*

- **a.** To the individual;
- **b.** For TPO [¶ E];
- **c.** Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the CE has complied with the applicable requirements of minimum necessary [¶ B.3and ¶ C.7], and safeguards [¶ K.3.c].
- **d.** Pursuant to an authorization [¶ G.];
- **e.** Pursuant to an agreement, or as otherwise permitted by 164.510 [¶ F.];
- **f.** As otherwise permitted pursuant to 164.502, 164.512, 164.514(e), (f), or (g) [¶¶ C, I].

2. Required Disclosures: CE is required to disclose PHI: *164.502(a)(2)*

- **a.** To individual pursuant to 164.524, 164.528 [¶¶ H.1, K.2];
- **b.** When required by the Secretary of HHS to investigate or determine CE's compliance with the regulations, [¶ L.4];
- **c.** When required by law, [¶¶ I.3 through I.6]

3. Disclosures by Whistleblowers and Workforce Member Crime Victims: *164.502(j)*

- **a.** CE has not violated use/disclosure restrictions if a member of its workforce or a BA discloses PHI provided that:
  - i. The workforce member or BA believes in good faith that the CE has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or the care, services, or conditions provided by the CE potentially endangers one or more patients, workers or the public; and
  - ii. The disclosure is to:
    1. a public health authority, health oversight agency, or healthcare accreditation organization authorized to investigate or oversee the conduct at issue, or

2. an attorney retained by the workforce member or BA for the purpose of determining legal options of the workforce member or BA with regard to the conduct.

b. CE has not violated use/disclosure restrictions if a member of the workforce who is the victim of a criminal act discloses PHI to a law enforcement officer, provided that: PHI disclosed is about the suspected perpetrator of the criminal act; and PHI disclosed is limited to the information listed in 164.512(f)(2)(i) [see ¶ I.6.b.i]

4. HIPAA Limited Data Set

164.514(e)
164.514(e)(1)

a. A CE may use or disclose a limited data set ("LDS") as long as the CE enters into a proper data use agreement [¶ C.4.b] for the use or disclosure of the LDS with the recipient and meets the following requirements:

i. CE may use or disclose LDS only for the purposes of research, public health, or health care operations;

ii. CE may use PHI to create a LDS, or disclose PHI to a BA to create a LDS, whether or not used by the CE; and

iii. An LDS is PHI that excludes the following listed direct identifiers of the individual, relatives, employer, or household members: *164.514(e)(2)*

1. Names
2. Postal addresses
3. Telephones numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical records numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate or license numbers
11. Vehicle identification numbers, including license plate numbers
12. Device and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers
16. Full face or likeness images

b. CE may use or disclose a LDS only if the CE obtains satisfactorily assurance in the form of a data use agreement that the recipient will only use or disclose the PHI for limited purposes. The data use agreement between the CE and LDS Recipient must: *164.514(e)(4)*

i. Establish the permitted uses or disclosures of the LDS that are consistent with the limitation it be used only for research, public health, or health care operations;

ii. The data use agreement cannot authorize the Recipient to use or disclose the LDS in a manner that the CE could not pursuant to this subpart;

iii. Establish who is permitted to use or disclose the LDS; and

iv. Require the Recipient:

1. Not to use or disclose the information other than as permitted by the Agreement or as required by law.
2. Use appropriate safeguards to prevent the use or disclosure of the LDS other than provided for by the Agreement.
3. Report any breach of the agreement to the CE.
4. To hold its agents and subcontractor to the same obligations the Recipient has pursuant to the Agreement.
5. Not identify or re-identify the information in the LDS or contact the individuals whose information is in the LDS.

c. A CE must take steps to address violations of the Recipient. *164.514(e)(4)(iii)*

i. A CE is not in compliance if it is aware the Recipient has a pattern of activity or practice that is a material breach of the data use agreement, unless:

1. The CE took reasonable steps to cure or end the violation; and
2. if such steps were unsuccessful discontinued the disclosure of PHI to the Recipient and reported the problem to the Secretary of HHS.

ii. A Recipient who breaches a data use agreement and is a CE, is also noncompliant with the standards, implementation specifications, and requirements of 164.514(e) [¶ C.4].

5. Uses or Disclosures for Fundraising: *164.514(f)*

a. CE may use or disclose to a BA or to an institutionally related foundation the following PHI for the purpose of raising funds for its own benefit without authorization pursuant to 164.508 [¶ G]:

i. Demographic information relating to individual; and

ii. Dates of health care provided to individual.

b. Requirements for use/disclosure for fundraising:

i. CE may not use/disclose PHI for fundraising purposes unless CE's privacy notice includes a statement required by 164.520(b)(1)(iii)(B) [see ¶ D.2.c.ii]

ii. CE must include in any fundraising materials sent a description of how to opt out of receiving further communications.

iii. CE must make reasonable efforts to ensure that individuals who opt out of receiving communications are not sent such communications.

6. Uses or Disclosures for Underwriting and Related Purposes: *164.514(g)*

If a health plan receives PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal or

replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such PHI for any other purpose, except as required by law.

7. Minimum Necessary: When using or disclosing PHI or when requesting PHI from another CE, a CE must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. *164.502(b)*

a. Minimum necessary standard does not apply to: *164.502(b)(2)*

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

ii. Uses or disclosures made to the individual, or pursuant to an authorization [¶ G];

iii. Uses/disclosures required by law under 164.512(a) [¶ I.3], and;

iv. Uses/disclosures required for compliance with applicable parts of the privacy regulations.

b. Implementing standard for minimum necessary uses of PHI: *164.514(d)(2)*

i. CE must identify those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and

ii. For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

iii. CE must make reasonable efforts to limit the access of such persons or classes identified above to PHI consistent with the categories described above.

c. Implementing standard for minimum necessary disclosures of PHI: *164.514(d)(3)*

i. For any type of disclosure that it makes on a routine and recurring basis, a CE must implement policies and procedures (which may be standard protocols) that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, a CE must: develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought, and; review requests for disclosure on an individual basis in accordance with such criteria.

ii. CE may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

1. Making disclosures to public officials that are permitted under 164.512 [¶ I], if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

2. The information is requested by another CE;

3. The information is requested by a professional who is a member of its workforce or is a business associate of the CE for the purpose of providing professional services to the CE, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

4. Documentation or representations that comply with the applicable requirements of 164.512(i) [¶ I.8] have been provided by a person requesting the information for research purposes.

d. Implementing standard for minimum necessary requests for PHI: *164.514(d)(4)*

i. CE must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other CEs;

ii. For a request that is made on a routine and recurring basis, CE must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made;

iii. For all other requests, CE must develop criteria designed to limit the request to the information reasonable necessary to accomplish the purpose for which the request was made; and review requests for disclosure on an individual basis in accordance with such criteria.

e. Requests for the entire record: For all uses, disclosures, or requests to which the requirements of ¶ C.7 apply, a CE may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. *164.514(d)(5)*

8. PHI of Deceased Individuals: CE must comply with requirements of the privacy regulations with respect to PHI of deceased individuals. *164.502(f)*

9. Personal Representatives: Except as provided in ¶¶ C.9.b and C.9.d, CE must treat a personal representative as the individual. *164.502(g)*

a. Adults and emancipated minors: If under applicable law, a person has authority to act on behalf of an adult or emancipated minor in making health care decisions, CE must treat the person as a personal representative with respect to PHI relevant to such representation.

b. Unemancipated minors: If under applicable law, a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an unemancipated minor in making health care decisions, CE must treat the person as a personal representative with respect to PHI relevant to such representation, except that person may not be a personal representative and the minor may act as an individual with respect to PHI pertaining to health care if:

i. Minor consents to such health care services, and no other consent is required by law (regardless of whether another person's consent has been obtained), and the minor has not requested that another person to be treated as the personal representative;

ii. Minor may lawfully obtain health care service without consent of parent, guardian, or other person acting in loco parentis and consent (by the minor, or court, or another legally authorized person) has been obtained;

iii. Parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between health care provider and the minor; ¶ C.9.b.iv.

iv. Notwithstanding the provisions contained in ¶ C.9.b through ¶ C.9.b.iv: (1) if and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a CE may disclose, or provide access in accordance with ¶ H.1 to, PHI about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; (2) if, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a CE may not disclose, or provide access in accordance with ¶ H.1 about an unemancipated minor to a parent, guardian or other person acting in loco parentis; and; (3) where the parent, guardian, or other person acting in loco parentis is not the personal representative under ¶ C.9 and where there is no applicable access provision under state or other law, including case law, a CE may provide or deny access under ¶ H.1 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in exercise of professional judgment. *164.502(g)(3)(ii)*

c. Deceased individuals: If under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or his/her estate, CE must treat the person as a personal representative with respect to PHI relevant to such representation. *164.502(g)(4)*

d. Abuse, neglect, and endangerment situations: Notwithstanding a state law or any requirement of ¶ C.9.d to the contrary, CE may elect not to treat a person as a personal representative of an individual if: *164.502(g)(5)*

i. CE has reasonable belief that individual has been or may be subjected to domestic violence, abuse or neglect by such person, or treating such person as the personal representative could endanger the individual, and

ii. CE, in exercise of professional judgment, decides it is not in the best interest of the individual to treat the person as the personal representative.

10. De-identification of PHI:

a. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that such *164.514(a)*

information can be used to identify an individual is not individually identifiable health information.

b. Requirements for de-identification of PHI: CE may determine that health information is not individually identifiable health information only if: *164.514(b)*

i. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: Applies these principles and methods and determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and documents the methods and results of the analysis that justify such determination;

Or

ii. The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed, and the CE does not have actual knowledge that the information could be used alone, or in combination with other information to identify an individual who is the subject of the information:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (i) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (ii) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;

- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code except as permitted by ¶ C.9.c (re-identification).

And

iii. The CE does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

c. Re-identification: CE may assign a code or other means of record identification to allow information deidentified under this section to be re-identified by the CE, provided that: *164.514(c)*

i. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

ii. CE does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

D. NOTICE OF PRIVACY PRACTICES/PRIVACY NOTICE: *164.520*

1. Notice to Individuals Required: An individual has a right to adequate notice of: the uses and disclosures of PHI that may be made by the CE, and; of the individual's rights and the CE's duties with respect to PHI except: *164.520(a)*

a. An inmate has no right to notice and these notice provisions do not apply to a correctional institution.

b. An individual enrolled in a Group Health Plan (GHP) has a right to notice:

i. From the GHP if the individual does not receive health benefits under the GHP through an insurance contract with a health insurance issuer or HMO; or

ii. From a health insurance issuer or HMO with respect to the GHP through which such individual receives his/her health benefits.

c. A GHP that provides health benefits solely through an insurance contract with a health insurance issuer or HMO and that creates or receives PHI or information on whether an individual is participating in the GHP, or is enrolled or has disenrolled from a health insurance issuer or HMO offered by the plan must:

i. Maintain a notice; and

ii. Provide notice to any person upon request.

d. A GHP that provides health benefits solely through an insurance contract with a health insurance issuer or HMO and does not create or receive PHI other than summary health information or information on whether an individual is participating in the GHP or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan is not required to maintain or provide the notice.

2. Content of Notice: Notice must be written in plain language and contain the following elements: *164.520(b)(1)*

a. The following statement must be displayed as a header or otherwise prominently: "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."

b. Uses and Disclosures: notice must contain:

i. A description, including at least one example, of the types of uses and disclosures the CE is permitted to make for purposes of TPO;

ii. A description of each of the other purposes the CE is permitted or required to use or disclose PHI without an individual's consent or authorization;

iii. Descriptions of uses and disclosures must reflect more stringent law, if applicable;

iv. Descriptions must contain sufficient detail to place an individual on notice of the uses and disclosures permitted or required;

v. A statement that other uses or disclosures will be made only with the individual's written authorization and the individual may revoke such authorization as provided by 164.508(b)(5) [¶ G.3.f];

c. Separate Statement for Certain Uses or Disclosures Required: If CE intends to engage in any of the following activities, the description of uses/disclosures for TPO must include a statement, as applicable, that:

i. CE may contact individual for appointment reminders, information about treatment alternatives or other health benefits that may be of interest to the individual;

ii. CE may contact individual to raise funds for the CE; or

iii. A GHP, or a health insurance issuer or HMO with respect to a GHP, may disclose PHI to the sponsor of the plan.

d. Individual Rights: Must include a statement of the individual's rights with respect to the PHI and a brief description of how to exercise those rights, as follows:

i. Right to request restriction on certain uses/disclosures pursuant to 164.522(a) [¶ H.2.a], and statement CE not required to agree to restriction;

ii. Right to receive confidential communications of PHI pursuant to 164.522(b) [¶ H.2.b];

iii. Right to inspect and copy PHI pursuant to [¶ H.1.a.];

iv. Right to amend PHI pursuant to 164.526 [¶ H.3.];

v. Right to receive accounting of disclosures pursuant to 164.528 [¶ K.2]; and

vi. Right to obtain paper copy of the notice upon request.

e. CE's Duties: Notice must contain:

i. Statement that CE is required by law to maintain privacy of PHI and to provide individuals with notice of its legal duties and privacy policies with respect to PHI;

ii. Statement that CE is required to abide by the terms of the notice currently in effect; and

iii. For a CE to apply a change in a privacy practice described in the notice affecting PHI created or received prior to issuing a revised notice, a statement that the CE reserves the right to change terms of its notice and to make new notice provisions effective for all PHI that it maintains, and a description of how it will provide individuals with the revised notice.

f. Complaints: Notice must contain a statement that individuals may complain to the CE and to the Secretary of HHS about privacy rights violations, describe how the individual may file a complaint with the CE, and a statement that the individual will not be retaliated against for filing a complaint.

g. Contact: Notice must contain name, or title, and telephone number of person or office to contact for further information [¶ K.3.a.ii];

h. Effective date: Notice must contain the date on which notice is first effective, which may not be earlier than date printed or published.

i. Optional Elements for Notice: If CE elects to limit the uses/disclosures that it is permitted to make under the regulations, the CE may describe its more limited uses/disclosures in its notice, but may not include a limitation affecting its right to make a use/disclosure required by law or permitted under 164.512(j)(1)(i) [¶ I.7]. In order for a CE to apply a change to its more limited uses/disclosures to PHI received prior to issuance of a new notice, the notice must include the statement permitting the CE to revise the notice as set forth in ¶ D.2.e.iii. *164.520(b)(2)*

j. Revisions to Notice: CE must promptly revise and distribute its notice whenever there is a material change to the uses/disclosures, the individual's rights, the CE's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflecting the change [¶ D.2.h]. *164.520(b)(3)*

3. Provision of Notice: CE must make the notice available on request to any person and to individuals specified hereunder, as applicable. *164.520(c)*

a. Health plans (not including group health plans described in ¶ D.1.c): *164.520(c)(1)*

i. Must provide notice:

1. No later than the compliance date for the health plan, to individuals then covered by the plan;
2. Thereafter, at the time of enrollment, to individuals who are new enrollees; and
3. Within sixty (60) days of a material revision of the notice to individuals then covered by the plan.

ii. No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

iii. Health plan satisfies ¶ D.3.a.i. by providing notice to the named insured of policy under which coverage is provided to the named insured and dependent(s).

iv. If health plan has more than one notice, ¶ D.3.a.i. is met by providing the notice relevant to the insured.

b. Providers with a direct treatment relationship with individual must: *164.520(c)(2)*

i. Provide notice no later than the first service delivery, including electronically delivered services, after the compliance date or in an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation;

ii. Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice, and if not obtained, document its good faith efforts to obtain and reason why acknowledgement was not obtained;

iii. If provider maintains a physical delivery site:

1. Have notice available at delivery site for individuals to request to take with them;
2. Post notice in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read it; and

iv. Upon revision of the notice, make it available upon request on or after the effective date and promptly comply with ¶ D.3.b.ii, if applicable.

c. Requirements Specific to Electronic Notice: *164.520(c)(3)*

i. CE that maintains a web site providing information about the CE's customer services or benefits must prominently post its notice on the web site and make it available electronically through the web site.

ii. CE may provide notice to an individual by email if the individual agrees to electronic notice and such agreement has not been withdrawn. If CE knows that email transmission has failed, a paper copy of notice must be provided to the individual. Provision of electronic notice is timely when it complies with ¶¶ D.3.a or D.3.b.

iii. If first service delivery to individual is electronic, provider must provide notice automatically and contemporaneously in response to individual's first request for service.

iv. Individual who receives electronic notice retains right to obtain paper copy upon request.

4. Joint notice by separate CEs: CEs that participate in an organized health care arrangement [¶ J.1.e] may provide joint notice provided that: *164.520(d)*

a. CEs involved agree to abide by the terms of the notice as part of participation in the organized health care arrangement;

b. Joint notice meets the requirements of ¶ D. 2, except that statements may reflect that notice covers more than one entity; and

i. Describes with reasonable specificity the CEs, or class of entities, to which the joint notice applies;

ii. Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies;

iii. If applicable, states that the participating CEs will share PHI with each other, as necessary, to carry out TPO

c. Participating CEs must provide notice to individuals in accordance with applicable specifications in ¶ D.3. Provision of the joint notice to an individual by any one of the participating CEs will satisfy the provisions of ¶ D.3 with respect to all other participating CEs.

5. Documentation: CE must document compliance with notice requirements by retaining copies of notices issued by the CE and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with ¶ D.3.b.

E. TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS (TPO) *164.506*

1. CE may use or disclose PHI for TPO set forth in ¶ E.1.b, provided that such use or disclosure is consistent with other applicable requirement of these privacy rules. *164.506(a)*

a. Standard: Consent *164.506(b)*

i. A CE may obtain consent of the individual to use or disclose PHI to carry out TPO.

ii. Consent shall not be effective when an authorization is required or when another condition must be met for such use and disclosure to be permissible under the Privacy Rules.

b. Implementation: TPO *164.506(c)*

i. CE may use or disclose PHI for its own TPO.

ii. CE may disclose PHI for treatment activities of a provider.

iii. CE may disclose PHI to another CE or provider for the payment activities of an entity that receives the information.

iv. CE may disclose PHI to another CE for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is:

1. for the purposes listed in ¶¶ A.15.a, A.15.b; or

2. for the purpose of health care fraud and abuse detection or compliance.

v. CE that participates in an organized health care arrangement may disclose PHI about an individual to another CE that participates in the organized health arrangement for any health care operations activities of the organized health care arrangement.

F. USES/DISCLOSURES REQUIRING OPPORTUNITY TO AGREE OR TO OBJECT *164.510*

: CE may use/disclose PHI provided the individual is informed in advance and has the opportunity to agree to or to prohibit or restrict the use or disclosure in accordance with the requirements of ¶ F.

1. Facility Directories: Except when an objection is expressed pursuant to ¶¶ F.1.b. or F.1.c., provider may:

a. Use the following PHI to maintain a directory for its facility, and disclose the information to clergy, and (except religious affiliation) to persons who ask for the individual by name: *164.510(a)(1)*

i. Individual's name;

ii. Individual's location within the facility;

iii. Individual's condition, in general terms, that does not communicate specific medical information, and

iv. Individual's religious affiliation.

b. Opportunity to object: Provider must inform an individual of the PHI it may include in the directory and the persons to whom the PHI may be released and provide the individual with the opportunity to prohibit or restrict some or all of such uses/disclosures as permitted in ¶ F.1. *164.510(a)(2)*

c. Emergency circumstances: If, due to individual's incapacity or an emergency treatment circumstance, the provider cannot, practicably provide the individual an opportunity to object to the use/disclosure of directory PHI, the provider may use or disclose some or all of the directory PHI if disclosure is: *164.510(a)(3)*

i. Consistent with individual's prior expressed preference, if any, that is known to the provider; and

ii. In the best interest of the individual, as determined by the provider, exercising professional judgment.

iii. Provider must inform the individual and provide the individual an opportunity to object to uses or disclosures when it becomes practicable to do so.

2. Uses/Disclosures to Those Involved in Individual's Care, or for Notification Purposes: *164.510(b)*

a. Permitted uses/disclosures: *164.510(b)(1)*

i. CE may, in accordance with ¶¶ F.2.b. and F.2.c., disclose to a family member, other relative, close personal friend of the individual, or any other person identified by individual, the PHI directly relevant to such person's involvement with or payment related to the individual's health care;

ii. CE may, in accordance with ¶¶ F.2.b., F.2.c., and F.2.d., use/disclose PHI to notify or assist (including identifying and locating) in the notification of a family member, personal representative, or another person responsible for care of the individual, of the individual's location, general condition, or death.

b. If individual is present or available (prior to use/disclosure), and has capacity to make health care decisions, CE may use/disclose PHI if it: *164.510(b)(2)*

i. Obtains individual's agreement;

ii. Provides individual with opportunity to object and individual does not object; or

iii. CE, in exercise of professional judgment, reasonably infers from the circumstances that the individual does not object.

c. If individual is not present, or opportunity to agree or object cannot practicably be provided due to incapacity or emergency circumstance, CE may, in exercise of professional judgment, determine whether disclosure is in the best interests of individual, and, if so, disclose only PHI that is directly relevant to person's involvement with individual's health care, including picking up filled prescriptions, x-rays, medical supplies, or other similar forms of PHI. *164.510(b)(3)*

d. CE may use/disclose PHI to public or private entity authorized by law or by its charter to assist in disaster relief efforts, for purpose of coordinating with such entities the uses or disclosures permitted by ¶ F.2.a.ii. The *164.510(b)(4)*

requirements of ¶¶ F.2.b. and F.2.c. apply to such uses/disclosures to extent that CE, in exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

G. AUTHORIZATION: *164.508*

1. Authorization Requirement: *164.508(a)(1)*

Except as otherwise permitted or required under the privacy regulations, CE may not use or disclose PHI without a valid authorization, and may only use/disclose PHI consistent with such authorization. *164.508(a)(2)*

a. Psychotherapy notes: CE must obtain authorization for any use/disclosure of psychotherapy notes, except:

i. For the following TPO:

1. Use by originator of notes for treatment;
2. Use/disclosure by CE for conducting its own counseling training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling; or
3. Use/disclosure by CE to defend itself in a legal action or other proceeding brought by the individual;

ii. Use/disclosure: to Secretary of HHS regarding compliance; as required by law; for health oversight activities with respect to the oversight of the originator of notes; to coroners and medical examiners, or; to avert serious threat to health or safety.

2. Authorization Required - Marketing: *164.508(a)(3)*

a. A CE must obtain an authorization for any use or disclosure of PHI for marketing, except of the communication is in the form of:

i. A face-to-face communication made by a CE to an individual; or

ii. A promotional gift of nominal value provided by the CE.

b. If the marketing involves direct or indirect remuneration to the CE from a third-party, the authorization must state that such remuneration was involved.

3. General Requirements for Authorization: *164.508(b)*

a. Must meet requirements specified in ¶¶ G.2.b (marketing), G.4 (core elements) and G.5 (required statements);

b. May contain additional elements or information, provided they are not inconsistent with required elements;

c. Authorizations with following defects are not valid:

i. Expired date, or expiration event known by CE to have occurred;

ii. Incompletely filled out with regards to required core element (See ¶ G.4);

iii. Known by CE to have been revoked;

iv. Violates restrictions on Compound authorizations ¶ G.3.d or Conditioning authorizations ¶ G.3.e;

v. Authorization is known by CE to contain false material information.

d. Compound authorizations: Authorization may not be combined with any other document, including any other written legal permission from the individual, except as follows: *164.508(b)(3)*

i. Authorization for use/disclosure of PHI for a research study may be combined with any other written permission for the same research study, including another authorization for such research or consent to participate in such research;

ii. Authorization for use/disclosure of psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes.

iii. Authorizations other than for use or disclosure of psychotherapy notes may be combined with any other such authorization, provided that the CE has not conditioned the provision of treatment, payment, enrollment in health plan, or eligibility for benefits on obtaining the authorization.

e. Conditioning Authorization: CE may not condition provision of treatment, payment, enrollment in health plan, or eligibility for benefits on provision of authorization except: *164.508(b)(4)*

i. Provider may condition provision of research-related treatment on provision of an authorization for such research;

ii. Health plan may condition eligibility for benefits and enrollment in the health plan prior to an individual's enrollment if the authorization is not for use or disclosure of psychotherapy notes and is sought 1) for eligibility or enrollment determinations or 2) for its underwriting or risk-rating determinations;

iii. May condition the provision of health care that is solely for the purpose of creating PHI for disclosure to 3rd party on provision of an authorization for disclosure of the PHI to such 3rd party.

f. Revocation: An individual may revoke an authorization at any time, in writing, except to the extent that CE has taken action in reliance thereon, or if authorization was obtained as a condition of obtaining insurance coverage and other law provides insurer right to contest claim under the policy or the policy itself. *164.508(b)(5)*

g. Documentation: CE must document and retain signed authorizations for period of six years from last effective date. [¶ K.3.j]. *164.508(b)(6)*

4. Core Elements: A valid authorization must contain at least the following elements: *164.508(c)*

a. Description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

b. Name of the person(s) or class of persons authorized to use or disclose the PHI;

c. Name of the person(s) or class of persons to whom the CE is authorized to make the use or disclosure;

d. Description of each purpose of the requested use/disclosure. Statement "at the request of the individual" is sufficient when an individual initiates the authorization and does not, or elects not to, provide a statement of purpose.

e. Expiration date or an expiration event that relates to the individual or the purpose of the use/disclosure. Statement "end of research study," "none," or similar language is sufficient is authorization is for research, including the creation and maintenance of a research database or research repository.

f. Signature of individual and date; If signed by personal representative, a description of the representative's authority to act for the individual;

5. Required Statements: In addition to the required elements, the authorization must contain statements adequate enough to place individual on notice of all of the following:

164.508(c)(2)

a. Individual's right to revoke authorization in writing and either: 1) exceptions to the right to revoke and a description of how the individual may revoke; or 2) reference to the CE's privacy notice [see ¶ D] if it contains the exceptions and description of how to revoke.

b. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization by stating either 1) CE may not condition treatment, payment, enrollment or eligibility for benefits on whether individual signs authorization when the prohibition on conditioning authorizations applies [¶ G.3.e] ; or 2) the consequences to the individual of a refusal to sign when, in accordance with ¶G.3.e, the CE can condition on failure to obtain such authorization.

c. The potential for information disclosed pursuant to the authorization to be subject to redisclosure by recipient and no longer protected by the HIPAA privacy rules.

6. Additional Requirements

164.508(c)(3)

a. Must be in plain language.

164.508(c)(4)

b. Copy to the individual of signed authorization.

H. INDIVIDUAL'S RIGHTS RELATED TO PHI:

1. Access of Individuals to PHI:

164.524

a. **Right of access**: An individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for: *164.524(a)(1)*

   i. Psychotherapy notes;

   ii. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

   iii. PHI maintained by a CE that is: subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), to the extent the provision of access to the individual would be prohibited by law; or exempt from CLIA.

b. **Denial of right of access without right of review**: A CE may deny an individual access without providing the individual an opportunity for review, in the following circumstances: *164.524(a)(2)*

   i. The PHI is excepted from the right of access [¶ H.1.a];

   ii. CE that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate;

   iii. An individual's access to PHI created or obtained by a covered health care provider in the course of research that includes treatment may be suspended while the research is in progress if the individual agreed to the denial of access when consenting to participate in the research, and the provider informed the individual that right of access will be reinstated upon completion of the research;

   iv. An individual's access to PHI contained in records subject to the Privacy Act (5 U.S.C. 552a) may be denied in accordance with the requirements of the Act;

   v. The PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

c. **Denial of right of access with right of review**: CE may deny an individual access, provided that the individual is given a right to have such denials reviewed, in the following circumstances: *164.524(a)(3)*

   i. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

   ii. The PHI makes reference to another person (not a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person, or;

iii. The request for access is made by the individual's personal representative and a The PHI makes reference to another person (not a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the individual or another person.

iv. If access is denied based on one of the grounds set forth in ¶¶H.1.c.i to H.1.c.iii, the individual has the right to have the denial reviewed by a licensed health care professional, designated by the covered entity to act as a reviewing official, who did not participate in the original decision to deny. The covered entity must promptly refer a request for review to the reviewing official, who must then determine, within a reasonable period of time, whether or not to deny the access requested based on the grounds set forth above. The covered entity must promptly provide written notice to the individual of the reviewing official's determination, and must provide or deny access in accordance with the determination. *164.524(a)(4); 164.524(d)(4)*

d. Requests for access; timely action: *164.524(b)*

i. CE must permit an individual to request access to inspect or to obtain a copy of the PHI about the individual that is maintained in a designated record set. CE may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

ii. CE must act on a request for access no later than 30 days after receipt of the request as follows:

1. If CE grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, as set forth in ¶ H.1.e;

2. If the CE denies the request, in whole or in part, it must provide the individual with a written denial, as set forth in ¶ H.1.f.

iii. If the request for access is for PHI that is not maintained or accessible to the CE on-site, the CE must act on the request no later than 60 days from the receipt of the request.

iv. If the CE is unable to act on the request within the appropriate time limit (30 or 60 days, as applicable), the CE may extend the time for such actions by no more than 30 days, provided that the CE, within the appropriate time limit, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the CE will complete its action on the request. The CE may have only one such extension of time for action on a request for access.

e. Provision of access: *164.524(c)*

i. CE must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the PHI about them in designated record sets. If the same PHI that is the subject of a request for access is maintained in

more than one designated record set or at more than one location, the CE need only produce the PHI once in response to a request for access.

ii. CE must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the CE and the individual.

iii. CE may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if:

1. The individual agrees in advance to such a summary or explanation; and
2. The individual agrees in advance to the fees imposed, if any, by the CE for such summary or explanation.

iv. CE must provide the access as requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request.

v. If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, the CE may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

1. Copying, including the cost of supplies and labor;
2. Postage; and
3. Preparing an explanation or summary of the PHI, if agreed to by the individual.

f. Denial of access:

164.524(d)

i. CE must provide a timely, written denial to the individual. The denial must be in plain language and must contain:

1. The basis for the denial;
2. If applicable, a statement of the individual's right to have the denial reviewed, including a description of how the individual may exercise such right; and
3. A description of how the individual may complain to the covered entity (pursuant to the complaint procedures set forth in ¶ K.3.d or to the Secretary of HHS pursuant to ¶ L.2. The description must include the name, or title, and telephone number of the contact person or office designated in ¶ K.3.a.ii.

ii. CE must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which the CE has a ground to deny access.

iii. If the CE does not maintain the PHI that is the subject of the individual's request for access, and the CE knows where the requested information is maintained, the CE must inform the individual where to direct the request for access.

g. Documentation: CE must document the following and retain the documentation for six years from the date of its creation: *164.524(e)*

i. The designated record sets that are subject to access by individuals; and

ii. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

2. Rights to Request Privacy Protection for PHI *164.522*

a. Right of an individual to request restriction of uses and disclosures: *164.522(a)*

i. CE must permit individual to request that CE restrict uses/disclosures for TPO and disclosures pursuant to ¶ F.2;

1. CE is not required to agree to the restriction;

2. If CE agrees to the restriction, it must not use or disclose the PHI in violation of the restriction except, if individual who made request is in need of emergency treatment and the restricted PHI is needed to provide that treatment, CE may use the restricted PHI or disclose it to a health care provider to provide such treatment;

3. Upon disclosure pursuant to ¶ H.2.a.i.2., CE must request that such health care provider not further use or disclose the PHI;

4. An agreed upon restriction is not effective to prevent uses or disclosures permitted or required under 164.502(a)(2)(i),164.510(a) or 164.512 [¶¶ C.2.a.; F.1; I].

ii. Terminating a restriction: CE may terminate its agreement to a restriction if:

1. The individual agrees to or requests the termination in writing;

2. The individual orally agrees to the termination, and agreement is documented; or

3. CE informs the individual that it is terminating its agreement to the restriction, except that termination is only effective as to PHI created or received after such notice.

iii. Documentation: CE that agrees to a restriction must document the restriction in accordance with ¶ K.3.j.

b. Confidential communications: *164.522(b)*

i. Requirements:

1. Provider must permit individuals to request (and must accommodate reasonable requests) to receive communications of PHI from the provider by alternative means or at alternative locations.

2. A health plan must permit individuals to request (and must accommodate reasonable requests) to receive communications of PHI from the health plan

by alternative means or at alternative locations if the individual clearly states that disclosure of the information could endanger the individual

ii. Conditions on providing confidential communications:

1. CE may require the individual to make a request for a communication to be made by alternative means or to an alternative location in writing;
2. CE may condition the provision of a reasonable accommodation on information as to how payment, if any, will be handled, when appropriate, and specification of an alternate address or method of contact;
3. A provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis;
4. A health plan may require that a request contain a statement that disclosure of the information to which the request pertains could endanger the individual.

3. Amendment of PHI:

164.526

a. Right to amend and denial of amendment:

164.526(a)(1)

i. Individual has the right to have CE amend PHI or other information in the designated record set for as long as CE maintains the record sets.

ii. CE may deny amendment request if it determines that the PHI or other record:

164.526(a)(2)

1. Was not created by the CE, unless the individual provides reasonable basis to believe that originator of PHI is no longer available to act on request;
2. Is not part of the designated record set;
3. Would not be available for inspection under ¶ H.1; or
4. Is accurate and complete.

b. Request for amendment and timely action:

164.526(b)

i. CE must permit an individual to request that the CE amend PHI maintained in the designated record set. CE may require request to be in writing and to provide reason/support for request, provided there is advance notice of these requirements.

ii. CE must act on request within 60 days of receipt, as follows:

1. If CE grants the request, in whole or in part, it must follow the requirements of ¶¶ H.3.c.i and H.3.c.ii. If it denies the request, in whole or in part, it must follow the requirements of ¶ H.3.d.
2. If CE needs more time to comply, it may obtain one extension for up to thirty days, provided that the CE notifies the individual in writing within the first 60 days of the reasons for delay and of the date by which action will be taken.

c. Accepting the amendment: If the CE accepts the requested amendment, in whole or part, it must: *164.526(c)*

i. Make the amendment by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment;

ii. Timely inform the individual that the amendment is accepted and obtain his/her identification of and agreement to have the CE notify relevant persons with which amendment needs to be shared pursuant to ¶ H.3.c.iii;

iii. Make reasonable efforts to inform and timely provide amendment to:

1. Persons identified by the individual as having received PHI and needing the amendment; and

2. Persons, including business associates, that the CE knows to have PHI that is the subject of the amendment and that may have relied, or could foreseeably rely on such information to the detriment of the individual.

d. Denying the amendment: If the CE denies the requested amendment, in whole or part, it must: *164.526(d)*

i. Provide the individual with a timely, written denial in plain language and containing:

1. The basis for the denial;, in accordance with ¶ H.3.a.ii;

2. Notice of individual's right to submit a written statement disagreeing with the denial, and information on how to file such statement;

3. Statement that, if individual does not submit a statement of disagreement, individual may request that CE provide individual's request and the denial with any future disclosures of the PHI that is subject of the request; and

4. Description of how individual may complain to CE pursuant to procedures described in ¶ K.3.d. (including name or title, and telephone number of contact person or office), or to the Secretary of HHS.

ii. Statement of disagreement: CE must permit the individual to submit to the CE a written statement disagreeing with the denial and the basis for disagreement. CE may reasonably limit the length of the statement.

iii. Rebuttal statement: CE may prepare a written rebuttal to the statement of disagreement. Whenever a rebuttal is prepared, CE must provide a copy to the individual.

iv. Record keeping: CE must, as appropriate, identify the record or PHI that is subject to the disputed amendment and append or otherwise link the request for amendment, the denial, any statement of disagreement, and any rebuttal to the designated record set.

v. Future disclosures:

1. If a statement of disagreement has been submitted, the CE must include the material appended in accordance with ¶ H.3.d.iv. or, at the election of the CE,

an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates.

2. If a statement of disagreement has not been submitted, the CE must include the request for amendment and the denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action in accordance with ¶ H.3.d.i.3.

3. When a subsequent disclosure is being made using a standard transaction under Part 162 of the regulations that does not permit additional material to be included, the CE must separately transmit the material required by ¶¶ H.3.d.v.1 or H.3.d.v.2, as applicable, to the recipient of the standard transaction.

e. A CE that is informed by another CE of an amendment to an individual's PHI pursuant to ¶ H.3.c.iii must amend the PHI in designated record sets as provided in ¶ H.3.c.i.

f. **Documentation**: CE must document the titles of the persons or offices responsible for receiving and processing requests for amendments and maintain documentation as required by ¶ K.3.j.

I. USES AND DISCLOSURES OF PHI FOR WHICH CONSENT, AUTHORIZATION, OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED

164.512

: A CE may use or disclose PHI without authorization or the opportunity to object in situations covered in this section ¶I.

1. Uses and Disclosures for Health Oversight Activities:

164.512(d)

a. Permitted disclosures: CE may disclose PHI to a health oversight agency for oversight activities authorized by law; including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

i. The health care system;

ii. Government benefit programs for which health information is relevant to beneficiary eligibility;

iii. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

iv. Entities subject to civil rights laws for which health information is necessary for determining compliance.

b. Exception to health oversight activities: For purpose of disclosures permitted pursuant to ¶ I.1.a, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and the investigation or other activity does not arise out of and is not directly related to:

i. The receipt of health care;

ii. A claim for public benefits related to health; or

iii. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

c. Joint activities or investigations: Notwithstanding ¶ I.1.b, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of ¶ I.1.

d. Permitted uses: If a CE is also a health oversight agency, the CE may use PHI for health oversight activities as outlined in ¶ I.1.

2. Uses and Disclosures for Public Health Activities: *164.512(b)*

a. Permitted disclosures: CE may disclose PHI for public health activities and purposes to:

i. A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

ii. A public health authority or other government authority authorized by law to receive reports of child abuse or neglect;

iii. 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 activities related to the quality, safety or effectiveness of such FDA regulated product or activity including:

1. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including use and labeling problems), or biological product;
2. To track FDA related;
3. Enable product recalls, repairs, or replacement or look back (including locating and notifying persons who have received products that have been recalled, withdrawn, or the subject of look back; or
4. To conduct post-marketing surveillance;

iv. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the CE or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

v. An employer, about an individual who is a member of the employer's workforce if:

The CE is a covered health care provider who is a member of the workforce of such employer or who provides a health care service to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace; or evaluate whether the individual has a work-related illness or injury;

1. The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
2. The employer needs such findings in order to comply with federal or state law to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and
3. The provider provides written notice (directly or posted) to the individual that PHI relating to the medical surveillance of the workplace and work-related illness and injuries is disclosed to the employer.

b. Permitted uses: If the CE is also a public health authority, the CE is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health.

3. Uses/Disclosures Required by Law: CE may use or disclose PHI to the extent such use/disclosure is required by law and the use/disclosure complies with and is limited to the relevant requirements of such law. CE must meet the requirements described in ¶¶ I.4 through I.6 for uses/disclosures required by law. *164.512(a)*

4. Uses/Disclosures Relating to Abuse and Neglect: *164.512(c)*

a. Permitted disclosures: Except for reports of child abuse or neglect covered under ¶ I.2.a.ii, CE may disclose PHI about an individual whom CE believes to be a victim of abuse, neglect, or domestic violence to a governmental authority authorized to receive such reports:

i. To extent the disclosure is required by law, and is limited to relevant requirements of that law;

ii. If the individual agrees; or

iii. To the extent the disclosure is expressly authorized by statute or regulation, and the CE believes, in the exercise of professional judgment that the disclosure is necessary to prevent serious physical harm to the individual or others, or, if the individual cannot agree due to incapacity, law enforcement or other public official authorized to receive the report represents that disclosure is not intended for use against the victim and that the law enforcement activity would be materially and adversely affected by waiting for the consent.

b. Informing the individual: CE that makes a disclosure permitted under ¶ I.4.a must promptly inform the individual that the report has been or will be made unless:

i. CE, in the exercise of professional judgment, believes that informing the individual would place the individual at risk of serious harm; or

ii. CE would be informing a personal representative whom the CE reasonably believes is responsible for the abuse, neglect, or other injury, and CE reasonably believes, in exercise of professional judgment, that informing such person would not be in the individual's best interests.

5. Uses/Disclosures for Judicial and Administrative Proceedings:

164.512(e)

a. CE may disclose PHI in the course of any judicial or administrative proceeding:

i. In response to an order of a court or administrative tribunal, but only the PHI expressly authorized for release by such order; or

ii. In response to a subpoena, discovery request or other lawful process not accompanied by a court or administrative order if:

1. CE receives satisfactory assurance, as described in ¶ I.5.a.iii, from the party seeking the PHI that reasonable efforts have been made to give the individual notice of the request; or

2. CE receives satisfactory assurance, as described in ¶ I.5.a.iv., from the party seeking the PHI that reasonable efforts have been made to secure a qualified protective order compliant with ¶ I.5.a.v.

iii. Satisfactory assurance that individual has been given notice may be met by provision of a written statement and accompanying documentation demonstrating that:

1. Party requesting the PHI has made a good faith attempt to provide written notice to the individual;

2. Notice includes sufficient information about the litigation or proceeding to permit the individual to raise an objection in the tribunal; and

3. The time to raise objections has lapsed and either no objection was filed or objections have been resolved in a manner consistent with disclosure.

iv. Satisfactory assurance that reasonable efforts have been made to secure a qualified protective order may be met by provision of a written statement and accompanying documentation demonstrating that the parties to the dispute have agreed to a qualified protective order and presented it to the tribunal, or the party seeking the PHI has requested a qualified protective order from the tribunal.

v. A qualified protective order means an order that prohibits the use or disclosure of PHI for any purpose beyond the litigation at hand, and requires that the PHI, and all copies, be returned to the CE or destroyed when the litigation is over.

vi. Notwithstanding ¶ I.5.a.ii, a CE may disclose PHI without the described assurances if the CE makes reasonable efforts to contact the individual as described in ¶ I.5.a.iii.or if it makes reasonable efforts to obtain a qualified protective order as described in ¶ I.5.a.iv.

b. Nothing in this section is meant to supersede or limit disclosures allowed by other sections.

6. Uses/Disclosures for Law Enforcement Purposes: CE may disclose PHI to law enforcement official for a law enforcement purpose if the conditions of ¶ I.6 are met, as applicable. *164.512(f)*

a. Permitted disclosures pursuant to process and as otherwise required by law: *164.512(f)(1)*

i. As required by law, including laws requiring reporting of certain types of wounds and injuries, except laws subject to ¶ I.2.a.ii. (re: reporting child abuse and neglect) and ¶ I.4.a.i; or

ii. In compliance with and as limited by relevant requirements of:

1. A court order, or a court ordered warrant, subpoena or summons issued by a judicial officer;
2. A grand jury subpoena; or
3. An administrative request, provided that the information is relevant to the law enforcement inquiry, the request is limited to the extent practicable, and de-identified information could not reasonably be used.

b. Permitted disclosure of limited information for identification and location purposes: Except for disclosures required by law as permitted under ¶ I.6.a, CE may disclose PHI in response to a law enforcement official's request to assist in identifying or locating a suspect, fugitive, material witness or missing person: *164.512(f)(2)*

i. CE may disclose only the following information:

1. Name and address;
2. Date and place of birth;
3. Social security number;
4. ABO blood type and rh factor;
5. Type of injury;
6. Date and time of treatment;
7. Date and time of death;
8. Distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

ii. Except as permitted under ¶ I.6.b.i, CE may not disclose for identification or location purposes any PHI relating to DNA or DNA analysis, dental records, typing, samples or analysis of body fluids or tissues.

c. Victims of Crime: Except for disclosures permitted under ¶ I.6.a, CE *164.512(f)(3)*

may disclose PHI in response to a law enforcement official's request relating to an individual who is or is suspected of being a victim of a crime, other than disclosures subject to ¶¶ I.2 and I.4, if:

i. Individual agrees; or

ii. CE is unable to obtain individual's agreement because of incapacity or other emergency provided that:

1. The law enforcement official needs the information to determine if someone else committed a crime, and the PHI will not be used against the victim;

2. Immediate law enforcement activity that depends on disclosure of the PHI would be materially and adversely affected by waiting; and

3. CE, exercising professional judgment, believes disclosure is in the best interest of the victim.

d. Decedents: CE may disclose decedent's PHI to law enforcement in order to alert law enforcement of the death if the CE suspects the death resulted from criminal conduct. *164.512(f)(4)*

e. Crime on Premises: CE may disclose PHI to law enforcement if the CE in good faith believes the PHI constitutes evidence of a crime committed on the premises of the CE. *164.512(f)(5)*

f. Reporting Crime in Emergencies: A covered provider, providing off-site emergency medical care may report PHI as necessary to alert law enforcement to the commission and nature of the crime; location of the crime and of crime victim(s); and the identity, description and location of the perpetrator. If CE believes that the emergency is the result of abuse, neglect or domestic violence, disclosure is subject to ¶ I.4. *164.512(f)(6)*

g. Correctional institutions and other law enforcement custodial situations: CE may disclose PHI to a correctional institution or to law enforcement official with custody of the individual when a correctional institution or law enforcement official represent that the PHI is necessary to provide care to the individual, or for the health and safety of the individual, other inmates, correctional employees, transport employees, law enforcement personnel at the location, and for the safety, security and good order of the institution. *164.512(k)(5)*

i. CE that is a correctional institution may use PHI for any purpose for which the PHI may be disclosed.

ii. An individual is no longer an inmate once released on parole, probation, supervised release or is otherwise no longer in lawful custody.

7. Uses and Disclosures to Avert a Serious Threat to Health or Safety: *164.512(j)*

a. CE may, consistent with applicable law and standards of ethical conduct, use or disclose PHI if the CE in good faith believes the use or disclosure is:

i. Necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

ii. Necessary for law enforcement authorities to identify or apprehend an individual:

1. Because of a statement by an individual admitting participation in a violent crime that the CE reasonably believes may have caused serious physical harm to the victim, or

2. Where it appears from all circumstances that the individual has escaped from a correctional institution or from lawful custody.

b. Use/disclosure not permitted: A use or disclosure pursuant to ¶ I.7.a.ii.1 may not be made if the information described therein is learned by the CE in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy; or through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.

c. Limit on information to be disclosed: A disclosure made pursuant to ¶ I.7.a.ii.1 shall contain only the statement described therein and the PHI described under ¶ I.6.b.i (disclosures for law enforcement for identification and location purposes).

d. A CE is presumed to have acted in good faith if its belief is based upon the CE's actual knowledge or reliance on a credible representation by a person with apparent knowledge or authority.

8. Uses and Disclosures for Research Purposes:

164.512(i)
164.512(i)(1)

a. CE may use/disclose PHI for research, regardless of source of funding, provided that:

i. CE obtains documentation that an alteration or waiver of the authorization required under 164.508 [¶ G] has been approved by either:

1. An Institutional Review Board (IRB) established under cited sections of the CFR, or

2. A Privacy Board that: (i) has members with varying backgrounds and appropriate professional competency to review the effect of the research protocol on privacy rights and related interests; (ii) includes at least one member who is not affiliated with the CE or the entity conducting or sponsoring the research, and is not related to anyone affiliated with these entities, and; (iii) does not have any member participating in a review of a project in which s/he has a conflicting interest.

ii. CE obtains from researcher representations that:

1. Use/disclosure is sought solely to review PHI to prepare a research protocol, or for a similar preparatory purpose;
2. No PHI will be removed from the CE; and
3. PHI sought is necessary for research purposes.

iii. For research on decedents' information, CE obtains from the researcher:

1. Representation that use/disclosure is sought solely for research on PHI of decedents;
2. Documentation of the death of individuals whose PHI is sought, upon request by the CE;
3. Representation that the PHI is necessary for research purposes.

b. Documentation supporting approval of alteration/waiver per 164.512(i)(1)(i) [¶ I.8.a.i] must include: *164.512(i)(2)*

i. Identification of approving board and date of approval;

ii. Statement that board determined that alteration/waiver satisfies the following criteria:

1. Use/disclosure of PHI involves no more than a minimal risk to the privacy of the individuals, based on, at least, the presence of the following elements:
   - Adequate plan exists to protect identifiers from improper use/disclosure;
   - Adequate plan exists to destroy identifiers unless there is justification for retention; and
   - Adequate written assurances given that PHI will not be used or disclosed other than as authorized for research study or otherwise under law.
2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably by conducted without access to and use of the PHI.

iii. A brief description of the PHI for which use or disclosure has been determined to be necessary by the IRB or privacy board has determined pursuant to ¶I.8.b.ii.3;

iv. Statement that the alteration/waiver was reviewed and approved as follows:

1. IRB must follow requirements of the Common Rule, including normal and expedited procedures (see cites in 164.512(i)(2)(iv)(A));
2. Privacy Board: normal review - must review at convened meetings where majority of members are present, including at least one member satisfying criteria of 164.512(i)(1)(i)(B)(2) [¶ I.8.a.i.2 (ii)] (at least one member not affiliated with CE or conduct/sponsorship of project}; alteration/waiver must be

approved by majority of members approved by majority of members present; or

3. Privacy Board: expedited review - may be used only if research involves no more than minimal risk to privacy; review and approval may be carried out by Chair, or one or more members as designated by Chair.

v. Documentation must be signed by Chair of approving IRB or Privacy Board, or by member designated by Chair.

9. Uses and Disclosures about Decedents: *164.512(g)*

a. Coroners and Medical Examiners: CE may disclose PHI to a coroner or medical examiner to identify a deceased person, determine the cause of death, or perform other functions authorized by law. A CE may use PHI for these purposes if it functions as a coroner or medical examiner.

b. Funeral Directors: CE may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry their duties. If necessary, PHI may be disclosed prior to, and in reasonable anticipation of, the individual's death.

10. Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes: *164.512(h)*

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

11. Uses and Disclosures for Specialized Government *164.512(k) 164.512(k)(1)*

a. Military and veterans activities:

i. CE may use/disclose PHI of armed forces personnel for activities deemed necessary by the appropriate military command authority to fulfill the military mission if notice has been published in the Federal Register that identifies the appropriate military command authorities and the purposes for which the PHI may be used or disclosed.

ii. CE that is a component of the Department of Defense or Department of Transportation may disclose PHI of a member of the armed services to the Department of Veterans Affairs (DVA) upon his or her discharge or separation from the military for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits.

iii. CE that is a component of DVA may use and disclose PHI to other components of DVA that determine eligibility for or entitlement to, or that provide, benefits.

iv. CE may use and disclose PHI of foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for U.S. armed services personnel.

b. National security and intelligence activities: CE may disclose *164.512(k)(2)*

PHI to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority.

c. **Protective services for the President and others**: CE may disclose PHI to authorized federal officials for the provision of protective services: *164.512(k)(3)*

   i. To the President and others designated under 18 U.S.C. 3056;

   ii. To foreign heads of state or others designated under 22 U.S.C. 2709(a)(3); or

   iii. For the conduct of investigations authorized by 18 U.S.C. 871 and 879.

d. **Medical suitability determinations**: CE that is a component of the Department of State may use PHI to make medical suitability determinations and may disclose results to officials in the Department of State who need access to it for the following purposes: *164.512(k)(4)*

   i. Required security clearance conducted pursuant to Executive Orders 10450 and 12698;

   ii. As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

   iii. For family to accompany a foreign service member abroad, consistent with sections 101(b)(5) and 904 of the Foreign Service Act.

e. **CEs that are government programs providing public benefits**: *164.512(k)(6)*

   i. Health plan that is a government program providing public benefits may disclose PHI relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such agencies or the maintenance of such information in a single or combined data system accessible to all such agencies is required or expressly authorized by statute or regulation.

   ii. CE that is a government agency administering a government program providing public benefits may disclose PHI relating to the program to another CE that is a government program providing public benefits if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions.

12. Disclosures for Workers' Compensation: CE may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs. *164.512(l)*

J. ORGANIZATIONAL REQUIREMENTS:

1. Relevant Definitions: *164.504(a)*

a. Common control exists if entity has power to directly or indirectly direct or influence the actions or policies of another entity.

b. Common ownership exists if entity(ies) possess ownership or equity interest of 5% or more of another entity.

c. Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with ¶J.3.c.iii and document this designation in accordance with ¶K.3.j.

d. Hybrid entity means a single legal entity that is a covered entity whose business activities include both covered and non-covered functions and that designates health care components in accordance with ¶J.1.c.

e. Organized health care arrangement means: *164.103*

i. A clinically integrated care setting in which individuals typically receive health care from more than one provider;

ii. An organized system of care in which multiple participating CEs:

1. Hold themselves out to the public as a joint arrangement; and

2. Participate in at least one of the following joint activities: (i) utilization review; (ii) quality assessment and improvement; or (iii) payment activities where there is shared financial risk;

iii. A group health plan and a health insurance issuer or HMO with respect to the plan, but only relating to PHI of participants or beneficiaries of the plan;

iv. Multiple group health plans maintained by the same plan sponsor; or

v. Multiple group health plans maintained by the same plan sponsor and health insurance issuers or HMOs with respect to such plans, but only relating to PHI of participants or beneficiaries of the plan.

f. Plan administration functions means administrative functions performed by the plan sponsor of a group health plan on behalf of that plan, and excludes functions performed by the sponsor in connection with any other benefit or plan of the sponsor.

g. Summary health information means information that may be individually identifiable health information and

i. That summarizes claims history, claims expenses, or types of claims relating to benefits under a group health plan; and

ii. Which has been de-identified pursuant to 164.514(b)(2)(i) [¶ C.10.b.ii], except that geographic information need only be aggregated to the level of a five digit zip code.

2. Health Care Component: If a CE is a hybrid entity, except as specified in ¶ J, the regulations apply only to the health care component *164.504(a)(1)*

of the entity.

3. Hybrid Entities: *164.504(a)(2)*

a. Applicability of other provisions of the regulations to hybrid entities:

i. Reference to a CE refers to the health care component of the CE;

ii. Reference to "health plan," "covered health care provider," or "health care clearinghouse" refers to health care component of CE if the component performs the functions of a health plan, covered health care provider or health care clearinghouse; and

iii. Reference to "protected health information" refers to PHI that is created or received by or on behalf of the health care component of the CE.

iv. Reference to “electronic protected health information” refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

b. Safeguard requirements: Hybrid entity must ensure that its health care components comply with applicable requirements of the regulations, including:

i. Health care component does not disclose PHI to another component of the CE, if such sharing would not be permitted if the two components were separate and distinct legal entities;

ii. Component acting as a "business associate" does not use/disclose PHI it creates or receives from or on behalf of the other component other than as permitted in its "business associate" type functions, and

iii. Workforce members who perform duties for both health care component(s) and other component(s) of CE must not use/disclose PHI created or received in the course of their work for the health care component in a way that is prohibited hereunder.

c. Responsibilities of hybrid entity:

i. Comply with compliance and enforcement requirements of Subpart C, Part 160 [¶ L.];

ii. Comply with implementation of policies and procedures required under 164.530(i) [¶ K.3.i]and safeguard provisions of 164.504(c)(2) [¶ J.3.b]; and

iii. Designate components that are part of one or more health care components of the CE and document the designations as required under 164.530(j) [¶ K.3.j], provided that, if the CE designates a health care component or provided that, if the CE designates a health care component or components, it must include any component that would meet the definition of CE if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs: covered functions or activities that would make such component a BA of

a component that performs covered functions if the two components were separate legal entities.

4. Affiliated Covered Entities: *164.105(b)(1)*

a. Legally separate CEs that are affiliated may designate themselves (including any health care component) as a single covered entity if all CEs so designated are under common ownership or control; such designation must be documented in accordance with 164.530(j) [¶ K.3.j].

b. Affiliated CE must ensure that its use and disclosure of PHI complies with applicable requirements of the regulations, and that if the affiliated CE combines functions of a health plan, a provider, or a health care clearinghouse, it complies with 164.504(g) [¶ J.7].

5. Disclosures to Business Associates (BAs): *164.502(e); 164.504(e)*

a. Standard for disclosures to BAs: CE may disclose PHI, or allow BA to create or receive PHI on CE's behalf, if CE obtains assurance that BA will safeguard the information; this standard does not apply with respect to:

i. Disclosure by CE to a provider concerning the individual's treatment;

ii. Disclosure by group health plan, or health insurance issuer or HMO with respect to the plan, when requirements of ¶ J.6 are met; or

iii. Uses/disclosures by health plan that is a governmental program providing public benefits, regarding PHI collected or shared for determination of eligibility or enrollment, where such information is collected, or eligibility or enrollment is determined, by an agency other than the one administering the plan, and such activity is authorized by law.

b. CE must document assurances through a written agreement or other arrangement meeting the following requirements: *164.502(e)(2); 164.504(e)*

i. Establish permitted and required uses/disclosures of PHI that are consistent with those authorized for the CE under the regulations, except that the contract/arrangement:

1. May permit BA to use/disclose PHI for management and administration of the BA: (i) if disclosure is required by law, or (ii) BA obtains reasonable assurances that the PHI will be held confidentially and used/disclosed only as required by law or for the purpose of the disclosure and person notifies BA of any breach of confidentiality; and

2. May permit BA to provide data aggregation services relating to the health care operations of the CE;

ii. Provide that the BA will:

1. Not use/disclose PHI except as authorized or as required by law;

2. Use safeguards to prevent unauthorized uses/disclosures;

3. Report unauthorized uses/disclosures to CE;
4. Pass on same obligations to subcontractors/agents;
5. Make PHI available for access and/or amendment by individuals in accordance with the provisions of 164.524 and 164.526 [¶¶ H.1 and H.3];
6. Make information available for provision of accounting of uses/disclosures [¶ K.2];
7. Make information available to the Secretary of HHS for purposes of determining CE's compliance with the regulations, and;
8. Return of destroy all PHI at termination of the contract, or offer ongoing protection for PHI.

iii. Authorize termination of the contract by the CE upon material breach by the BA.

c. If CE knows of a pattern or practice of material noncompliance by the BA, and reasonable steps have not cured breach, CE must do one of the following: *164.504(e)(1)*

i. Terminate the contract, if feasible; or

ii. Report the problem to the Secretary of HHS.

d. If CE and BA are both governmental entities, CE may comply with requirements of a BA agreement: *164.504(e)(3)(i)*

i. By entering into a Memorandum of Understanding covering the required terms; or

ii. If other law contains requirements applicable to the BA that satisfy the objectives of the terms.

e. If a BA is required by law to perform a function or activity or to perform a specified service on behalf of a CE, the CE may disclose PHI to the extent necessary to comply with that mandate, as long as CE documents an attempt to obtain the enumerated BA assurances and the reasons such assurances could not be obtained. *164.504(e)(3)(ii)*

f. CE may omit requirement for termination provision in contract if it would be inconsistent with statutory obligations of CE or BA. *164.504(e)(3)(iii)*

6. Group Health Plans: *164.504(f) 164.504(f)(1)*

a. Generally, in order for a group health plan to use or disclose PHI to the plan sponsor or to permit disclosure of PHI to the plan sponsor by a health insurance issuer or HMO for the plan, the group health plan must ensure that plan documents restrict uses and disclosures by the plan sponsor consistent with the requirements of the regulations, except when the use/disclosure:

i. Is made pursuant to the terms of an authorization pursuant to164.508 [¶ G]; or

ii. Involves summary health information disclosed to the plan sponsor in response to a request to use the information for the purposes of obtaining premium bids from

health plans for providing coverage under the group health plan or modifying, amending or terminating the group health plan. The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered plan.

b. Plan documents of a group health plan must be amended to incorporate provisions to: *164.504(f)(2)*

i. Establish permitted and required uses/disclosures of health information by the plan sponsor in keeping with the requirements of the regulations;

ii. Provide that the group health plan will not disclose PHI to the plan sponsor until receipt of a certification from the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

1. Only use or disclose the information as permitted or required by law;
2. Ensure that any agents/subcontractors agree to the same restrictions and conditions relating to PHI;
3. Not use/disclose PHI for employment related actions/decisions or in connection with other benefit or employee benefit plan of the plan sponsor;
4. Report to the group health plan any unauthorized uses/disclosures of which it becomes aware;
5. Make PHI available: for individual's access in accordance with 164.524 [¶ H.1], and for amendment in accordance with 164.526 [¶ H.3];
6. Make necessary information available for accounting of disclosures in accordance with 164.528 [¶ K.2];
7. Make internal practices and records relating to use/disclosure of PHI received from the group health plan available to Secretary of HHS for compliance review of group health plan;
8. If feasible, return or destroy all PHI received once no longer needed, and if not feasible to return or destroy, ensure that further use/disclosure is limited to purposes making return/destruction not feasible;
9. Ensure establishment of adequate separation pursuant to 164.504(f)(2)(iii) [¶ J.6.b.iii].

iii. Provide for adequate separation between the group health plan and the plan sponsor; plan documents must:

1. Describe employees or classes of employees or persons under control of plan sponsor to be given access to PHI; must include all employees or persons who

receive PHI relating to payment or other matters in the usual course of business;

2. Restrict access and use of PHI to plan administration functions performed on behalf of the group health plan, and;

3. Provide effective mechanism for resolving issues of noncompliance by such employees.

c. Uses and disclosures by group health plans: GHPs are: *164.504(f)(3)*

i. Permitted to disclose PHI to plan sponsor to carry out plan administration functions consistent with the provisions of 164.504(f)(2) [¶ J.6.b];

ii. Not to permit a health insurance issuer or HMO for the group health plan to disclose PHI to plan sponsor except as permitted hereunder;

iii. Not to disclose or permit health insurance issuer or HMO to disclose PHI to plan sponsor as otherwise permitted hereunder unless statement of such disclosure, as required by 164.520(b)(1)(iii)(C), is included in privacy notice [¶ D.2.c.iii];

iv. Not to disclose PHI to plan sponsor for purpose of employment related actions/decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

7. Requirements for CE with Multiple Covered Functions: CE *164.504(g)*

that performs multiple covered functions that would make the entity any combination of a health plan, a provider or a health care clearinghouse:

a. Must comply with the standards, requirements, and implementation specifications of the regulations as applicable to the covered functions performed, and;

b. May use or disclose PHI of individuals who receive the services of the health plan or provider, but not both, only for purposes related to the appropriate function being performed.

K. ADMINISTRATIVE REQUIREMENTS:

1. Verification Requirements: *164.514(h)* *164.514(h)(1)*

a. Prior to any disclosure permitted under the regulations, CE must:

i. Except with respect to disclosures under ¶ F, verify the identity of a person requesting PHI and the authority of such person to access the PHI if not known to the CE; and

ii. Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when it is a condition of the disclosure under the regulations.

b. Implementation requirements: *164.514(h)(2)*

i. Conditions on disclosure: If a disclosure is conditioned under the regulations on particular documentation, statements, or representations from the

person requesting the PHI, CE may rely, if reasonable under the circumstances, on documentation, statements or representations that, on their face, meet the applicable requirements.

1. The conditions in 164.512(f)(1)(ii)(C) [¶ I.6.a.ii.3] may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.
2. The documentation required by 164.512(i)(2) [¶ I.8.b] may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with the provisions 164.512(i)(2)(i)(v)[¶¶I.8.b.i and I.8.b.v].

ii. Identity of public officials: CE may rely, if reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of a public official:

1. If the request is made in person, presentation of agency identification badge, other official credentials, or other proof of government status;
2. If the request is in writing, on appropriate government letterhead;
3. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting with authority, or other evidence of agency, such as a contract for services, MOU, purchase order, that establishes that the person is acting on behalf of the public official;

iii. Authority of public officials: CE may rely, if reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

1. A written statement of legal authority under which the information is requested, or, if a written statement would be impractical, an oral statement of such authority;
2. A request made by legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

iv. Exercise of professional judgment: Verification requirements of ¶ K.1 are met if CE relies on the exercise of professional judgment in making a use or disclosure in accordance with 164.510 [¶ F] or acts on a good faith belief in making a disclosure under 164.512(j) [¶ I.7].

2. Accounting of Disclosures of PHI:

164.528
164.528(a)(1)

a. Right to an accounting of disclosures of PHI:

i. An individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

1. To carry out TPO as provided in ¶ C.1.b;
2. To individuals of PHI about them as provided in¶ C.1.a;
3. Incident to a use or disclosure otherwise permitted or required ¶K.2
4. Pursuant to an authorization as provided in ¶ G
5. For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in ¶ F;
6. For national security or intelligence purposes as provided in ¶ I.11.b;
7. To correctional institutions or law enforcement officials as provided in ¶ I.6.g; or
8. as part of a limited data set in accordance with ¶ C.10; or
9. That occurred prior to the compliance date for the CE.

ii. Suspension of right to accounting: *164.528(a)(2)*

1. CE must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided for in ¶ K.2.a.i, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
2. If the agency or official statement is made orally, the covered entity must: (i) document the statement, including the identity of the agency or official making the statement; (ii) temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and (iii) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to ¶ K.2.a.ii.1 is submitted during that time.

iii. An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

b. Content of the Accounting: CE must provide the individual with a written accounting that meets the following requirements: *164.528(b)*

i. Except as otherwise provided above, the accounting must include disclosures of PHI that occurred during the six years (or such shorter time period at the request of the individual) prior to the date of the request for an accounting, including disclosures to or by business associates of the CE.

ii. Except as otherwise provided by ¶¶ K.2.b.iii and K.2.b.iv the accounting must include for each disclosure:

1. The date of the disclosure;
2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed; and
4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement: (i) a copy of the individual's written authorization; or (ii) a copy of a written request for a disclosure, if any.

iii. If, during the period covered by the accounting, the CE has made multiple disclosures of 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:

1. The information required in ¶K.2.b.ii for the first disclosure during the accounting period;
2. The frequency, periodicity, or number of the disclosures made during the accounting period; and
3. The date of the last such disclosure during the accounting period.

iv. If, during the period covered by the accounting, the covered entity has made disclosures of PHI for a particular research purpose in accordance with ¶ I.8 for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, 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 protected health information that was disclosed; (4) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period; (5) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and (6) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity. (ii) If the covered entity provides an accounting for research disclosures, in accordance with this section, and if it is reasonably likely that PHI of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

164.528(b)(4)(i)

164.528(c)

c. Provision of the Accounting:

i. CE must provide the individual with the accounting requested no later than 60 days after receipt of the request; or

ii. If CE is unable to provide the accounting within 60 days after receipt of the request, the CE may extend the time to provide the accounting by no more than 30 days, provided that:

1. CE, within 60 days after receipt of the request, provides the individual with a written statement of the reasons for the delay and the date by which the CE will provide the accounting; and

2. CE may have only one such extension of time for action on a request for an accounting.

iii. CE must provide the first accounting to an individual in any 12 month period without charge. CE may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the CE informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

d. Documentation: CE must document the following and retain the documentation for six years from the date of its creation[¶K.3.j]: *164.528(d)*

i. The information required to be included in an accounting for disclosures of PHI that are subject to an accounting;

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

iii. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

3. Administrative Requirements: *164.530* *164.530(a)*

a. Required Personnel Designations: CE must designate, and document, according to ¶K.3.j, designations of:

i. Privacy Official: Responsible for development and implementation of the CE's policies and procedures, and

ii. Contact person or office: Responsible for receiving complaints under this section and able to provide information relating to the Privacy Notice [¶D].

b. Required Training: CE must train, and document the training of, all workforce members on policies and procedures relating to PHI as necessary and appropriate to their work functions, as follows: *164.530(b)*

i. To all workforce members by the applicable compliance date for the CE;

ii. To each new member of the workforce within a reasonable time upon joining the CE's workforce;

iii. To each workforce member whose functions are affected by a material change in policies or procedures required under the privacy regulations, within a reasonable time after the material change becomes effective.

c. **Safeguards to be in place**: CE must have in place appropriate administrative, technical and physical safeguards to reasonably safeguard PHI from intentional or unintentional unauthorized use or disclosure. The CE must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. *164.530(c)*

d. **Complaint Process**: CE must provide a process for individuals to make complaints about the CE's policies and procedures required by the privacy regulations and/or the CE's compliance with those policies and procedures, and must document all complaints received and disposition of same, if any. *164.530(d)*

e. **Sanctions to be in place**: CE must have, apply, and document application of appropriate sanctions against its workforce members who fail to comply with the CE's privacy policies and procedures or the requirements of the privacy regulations; NOTE: This standard does not apply to workforce members' actions meeting the requirements of the sections relating to disclosures by whistleblowers and workforce member crime victims [164.502(j)/¶ C.3], or intimidating and retaliatory acts [164.530(g)(2)/¶ K.3.g.ii]. *164.530(e)*

f. **Mitigation of harmful effects**: CE must mitigate, to extent practicable, any harmful effects that are known to the CE of unauthorized uses/disclosures of PHI in violation of its policies and procedures or the requirements of the privacy regulations by CE or BA. *164.530(f)*

g. **Intimidating or retaliatory acts prohibited**: CE may not intimidate, threaten, coerce, discriminate against or take other retaliatory action against: *164.530(g)*

   i. Any individual for exercise of any right or participation in any process established by the privacy regulations; or

   ii. Any individual or other person for: filing a complaint with the Secretary of HHS; testifying, assisting, or participating in investigation, compliance review, or proceeding/hearing under the regulations, or; engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under the regulations, as long as such opposition does not involve the disclosure of PHI in violation of privacy regulations.

h. **Waiver of Rights prohibited**: CE may not require individuals to waive any of their rights to file a complaint with the secretary of HHS or otherwise under these regulations as a condition of treatment, payment, enrollment, or eligibility for benefits. *164.530(h)*

i. **Necessary Policies and Procedures**: *164.530(i)*

   i. CE must design and implement policies and procedures relating to PHI to comply with requirements of the privacy regulations, taking into account the size and the types of activities that relate to PHI engaged in by the CE. (This

standard is not to be construed to permit or excuse an action that violates any other standard, implementation, specification, or other requirement of the privacy regulations.)

ii. Changes to Policies and Procedures:

1. CE must change its policies and procedures as necessary and appropriate to changes in the law/regulations. Whenever there is a change in law that necessitates a change to CE's policies and procedures, CE must promptly document and implement the revised policy or procedure; if the change materially affects the content of the Privacy Notice [¶ D.2], the CE must promptly make appropriate revisions to the notice in accordance with 164.520(b)(3) [¶ D.2.j].

2. When CE changes its privacy practices as stated in its Privacy Notice, and makes corresponding changes in policies and procedures, changes may be effective as to PHI created or received prior to the effective date of the policy/procedure changes and notice revision if its Privacy Notice includes a statement reserving the right to make changes in the CE's privacy practices. To implement change in privacy practice, and corresponding changes in policies/procedures, CE must ensure that revised policies and procedures comply with the regulations, document the revised policies and procedures, revise the Privacy Notice and make it available; changes to policies and procedures may not be implemented prior to the effective date of the revised notice.

3. If CE has not reserved right to change privacy practices, CE is bound by privacy practices as stated in Privacy Notice with regard to PHI created or received while notice is in effect; CE may change a privacy practice without having reserved the right to do so as long as the practice is in compliance with the regulations and is effective only with respect to PHI created or received after the effective date of the notice (¶D.2.h).

4. CE may change policies and procedures that do not materially affect the content of the Privacy Notice provided that the revised policies and procedures comply with the regulations and are properly documented.

j. Documentation Requirements: CE must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities, or designations that are required to be documented under the regulations, for a period of six years from the later of the date of creation or the last effective date. *164.530(j)*

k. Group Health Plans: To the extent that a group health plan provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and the plan does not create or receive PHI except for summary health information (defined in 164.504(a)/¶ J.1.g) or information on the *164.530(k)*

individual's participation in the plan, or enrollment and disenrollment from a health insurance issuer or HMO offered by the plan:

i. The group health plan is not subject to the provisions requiring personnel designations, training, safeguards, complaint process, sanctions, mitigation, and policies and procedures, described in ¶ K.3; and

ii. The group health plan is subject to the documentation standard only with respect to plan documents amended in accordance with 164.504(f) [relating to sharing of information among or between a group health plan, the plan sponsor, a health insurance issuer, and/or an HMO, see ¶ J.6]

L. COMPLIANCE AND ENFORCEMENT: *160.304*

1. Principles for Achieving Compliance:

a. Cooperation: Secretary of HHS will, to the extent practicable, seek cooperation of CEs in obtaining compliance with the regulations.

b. Assistance: Secretary of HHS may provide technical assistance to CEs to help them comply voluntarily with the regulations.

2. Complaints to the Secretary of HHS: *160.306*

a. Right to file complaint: A person who believes a CE is not complying with the regulations may file a complaint with the Secretary of HHS.

b. Requirements for filing complaint:

i. Complaint must be filed in writing, either on paper or electronically;

ii. Complaint must name entity that is the subject of the complaint and describe acts or omissions believed to be in violation of the regulations;

iii. Complaint must be filed within 180 days of when complainant knew or should have known of the act or omission, unless the time limit is waived by the Secretary of HHS for good cause shown.

c. Investigation: Secretary of HHS may investigate complaints, which may include review of policies, procedures, or practices of the CE and of the circumstances regarding the alleged acts or omissions.

3. Compliance Reviews: *160.308*

Secretary of HHS may conduct compliance reviews to determine whether CEs are complying with applicable requirements of the regulations.

4. Responsibilities of CEs: *160.310*

a. **Provide records and compliance reports**: CE must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary of HHS may determine to be necessary to enable the Secretary to ascertain whether CE has complied and is complying with the regulations.

b. Cooperate with complaint investigations and compliance reviews: CE must cooperate with the Secretary of HHS if the Secretary undertakes an investigation or compliance review of the policies, procedures or practices of a CE.

c. Permit access to information:

i. CE must permit access by the Secretary of HHS during normal business hours to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the regulations. If the Secretary determines that exigent circumstances exist, a CE must permit access at any time, without notice.

ii. If any of the information required of a CE hereunder is in the exclusive possession of another agency, institution, or person that fails or refuses to furnish the information, the CE must so certify, and set forth the efforts it undertook to obtain the information.

iii. PHI obtained by the Secretary of HHS in connection with an investigation or compliance review will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of the regulations.

5. Secretarial Action Regarding Complaints and Compliance Reviews: *160.312*

a. Resolution where noncompliance is indicated:

i. If an investigation or compliance review indicates a failure to comply, the Secretary of HHS will so inform the CE and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

ii. If the Secretary of HHS finds the CE is not in compliance and determines that the matter cannot be resolved informally, the Secretary may issue to the CE, and, if the matter arose from a complaint, the complainant, written findings documenting the noncompliance.

b. Resolution when no violation is found: If, after an investigation or compliance review, the Secretary of HHS determines that further action is not warranted, the Secretary will so inform the CE and, if the matter arose from a complaint, the complainant, in writing.

6. Improved Enforcement:

a. Willful Neglect: Generally, noncompliance due to will neglect is an enforceable violation of the HIPAA statute and regulations subject to penalty under Section 1176 of the Social Security Act (42 U.S.C. 1320d-5). HHS is required to formally investigate a complaint if a preliminary investigation of the facts of the complaint indicates a possible violation due to will neglect.

b. Enforcement by State Attorneys General

i. Except as otherwise provided, in cases where an attorney general of a state has reason to believe that the interest of one or more patients is threatened or adversely affected by a violation, the AG, as parens patriae, may bring a civil action in a U.S. District Court to enjoin further violation or to obtain damages on behalf of residents of the State.

ii. Calculation of Statutory Damages: Statutory damages shall be determined by multiplying the number of violations by up to $100.

1. In cases of continuing violations, the number of violations shall be determined consistent with HIPAA regulations.

2. Total damages imposed during a year for identical violations are capped at $25,000.

3. The court may consider the nature and extent of the violation and harm in assessing damages

iii. Assessment of Costs and Attorney Fees: In cases of successful action, the court has discretion to award costs and reasonable attorney fees to the State.

iv. Notice to the Secretary: The State shall serve prior written notice of any action upon the Secretary, including a copy of the complaint. If that is not feasible, the State shall serve on the Secretary immediately upon filing the complaint.

1. The Secretary shall have a right to intervene, be heard on all matters, and petition for appeal.

v. Venue: Any action brought by an attorney general under this section may be brought in the United States district court that meets applicable requirements relating to venue under 28 U.S.C. § 1391.

vi. Service of Process: In an action brought by an attorney general under this section, process may be served in any district in which the defendant lives or maintains a physical place of business.

vii. Limitation on State Action: No State Attorney General may bring an action if the Secretary has instituted an action with regard to a specific violation.

viii. Statute of Limitations: The same statute of limitations applies as would apply to an action for civil money penalties under the federal statute (see Section ___ below).

ix. Corrective Action: Amendments to the American Recovery and Reinvestment Act do not prevent Office for Civil Rights of the Department of Health and Human Services from using corrective action without penalty where the person did not know of the violation and would not have known with reasonable diligence.

7. Imposition of Civil Monetary Penalties:

160.404

a. Civil Penalty Amounts:

i. For violations occurring prior to February 18, 2009, the Secretary may not impose a civil penalty of more than $100 per violation or in excess of $25,000 for identical violations during a calendar year.

ii. For violations occurring on or after February 18, 2009:

1. If the violation was unknown and would not have been known with reasonable diligence, a penalty of at least $100 per violation, but not more than $50,000

per violation. The total amount imposed may not exceed $1.5 million during a calendar year for identical violations.

2. If the violation was due to reasonable cause but not willful neglect, a penalty of at least $1,000 per violation, not more than $50,000 per violation, shall be imposed. The total amount imposed may not exceed $1.5 million during a calendar year for identical violations.
3. If the violation was due to willful neglect, but it was corrected within 30 days of when it was known or would have been known by exercising reasonable diligence, a penalty of at least $10,000 per violation, but not more than $50,000 per violation, shall be imposed. The total amount imposed may not exceed $1.5 million during a calendar year for identical violations.
4. If the violation was due to willful neglect, and it was not timely corrected, a penalty of at least $50,000 per violation, capped at $1.5 million during a calendar year for identical violations, shall be imposed.

b. Violations of an Identical Requirement or Prohibition: *160.406*

i. The Secretary will determine the number of violations based on the nature of the Covered Entity's or Business Associate's obligation to act under the provision that is violated. In the case of a continuing violation of a provision, a separate violation occurs each day the Covered Entity or Business Associate is in violation of the provision.

c. Factors Considered in Determining the Amount of a Civil Monetary Penalty: *160.408*

i. In determining the amount of any civil money penalty, the Secretary may consider as aggravating or mitigating factors, as appropriate, any of the following:

1. The nature of the violation, in light of the purpose of the rule violated.
2. The circumstances, including the consequences, of the violation, including but not limited to:
   - The time period during which the violation(s) occurred;
   - Whether the violation caused physical harm;
   - Whether the violation hindered or facilitated an individual's ability to obtain health care; and
   - Whether the violation resulted in financial harm.
3. The degree of culpability of the covered entity, including but not limited to:
   - Whether the violation was intentional; and
   - Whether the violation was beyond the direct control of the covered entity.
4. Any history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, including but not limited to:
   - Whether the current violation is the same or similar to prior violation(s);
   - Whether and to what extent the covered entity has attempted to correct previous violations;

- How the covered entity has responded to technical assistance from the Secretary provided in the context of a compliance effort; and
- How the covered entity has responded to prior complaints.

5. The financial condition of the covered entity, including but not limited to:
   - Whether the covered entity had financial difficulties that affected its ability to comply;
   - Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity to continue to provide, or to pay for, health care; and
   - The size of the covered entity.
6. Such other matters as justice may require.

d. Affirmative Defenses: *160.410*

i. For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violations, including the following:

1. The violation is an act punishable under 42 U.S.C. 1320d–6;
2. The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the federal common law of agency, and, by exercising reasonable diligence, would not have known that the violation occurred; or
3. The violation is: due to reasonable cause and not willful neglect; and corrected during either:
   - The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or
   - Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

ii. For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violations, including the following:

1. The violation is an act punishable under 42 U.S.C. 1320d–6; or
2. The covered entity establishes to the satisfaction of the Secretary that the violation is:
   - Not due to willful neglect; and corrected during either:
   - The 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or
   - Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

e. Waiver: *164.412*

i. For violations due to reasonable cause and not willful neglect that are not corrected within the period described in §160.410(a)(3)(ii) or (b)(2)(ii), as applicable, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.

f. Limitations: *164.414*

i. No action under §160.400 et seq. may be entertained unless commenced by the Secretary, in accordance with §160.420, within 6 years from the date of the occurrence of the violation.

Not Covered: 45 CFR 416-426

g. Distribution of Civil Penalties:

i. A civil monetary penalty or settlement collected that relates to privacy or security violations shall be transferred to OCR to be used for enforcement purposes.

1. Not later than 8/17/10, the Comptroller General is to submit to HHS a report recommending a method by which an individual harmed by a violation may receive a percentage of the civil penalty or settlement. Note: HHS to promulgate regulations about the methodology by 2/17/12.

NOT COVERED: Transition Provisions [**164.532**]; Compliance Dates [**164.534**]

8. Notifications in case of breach of unsecured data – Pub L111-5 § 13401, 13402(a), (h) *164 Subpart D*

a. Applicability of Notice Requirement (13402(a), (h)) *164.400*

i. Was the data unsecured? – data is unsecured for these purposes if it is not rendered unusable, unreadable or indecipherable to unauthorized individuals according to the technologies/methodologies specified by the Secretary of HHS, as follows:

1. Electronic PHI has been encrypted by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key that has not been breached; decryption tools should be stored on device or at location separate from the data; valid encryption processes:

- Data at rest – consistent with NIST Special Publications 800-52, *Guide to Storage Encryption Technologies for End User Devices*
- Data in Motion – comply with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*, or others which are Federal Implementation Processing Standards (FIPS) 140-2 validated

2. Media on which data is stored or recorded has been destroyed the following ways:

- Paper, film or other hard copy has been shredded or destroyed such that PHI cannot be read or reconstructed; redaction is specifically excluded as means of destruction

- Electronic media have been cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization* such that PHI cannot be retrieved

ii. Was there a breach? – unauthorized acquisition, access, use or disclosure of PHI which compromises the security/privacy of the PH (13400) *164.402*

1. Breach specifically excludes:
   - Unintentional acquisition, access or use of PHI by a workforce member, agent or BA if made in good faith and within scope of authority and does not result in further unauthorized use or disclosure
   - Inadvertent disclosure by authorized person or BA to another person authorized to access PHI at the same CE, BA or organized health care arrangement that does not result in further unauthorized use or disclosure
   - Disclosure where CE or BA has a good faith belief that unauthorized person would not reasonably have been able to retain such information
2. PHI includes data in any form; includes limited data sets but does not include de-identified data or categories of individually identifiable health information otherwise excluded under the regulations, i.e. employment records; additional, narrow exclusion of limited data sets if dates of birth and zip codes are also excluded from the data set
3. Unauthorized use or disclosure specifically defined as impermissible use or disclosure under subpart E of the regulations; terms "acquisition" and "access" deemed to be included within meaning of terms "use" and "disclosure" [definition of "access" at 164.304 limited to that subpart]
4. CE to perform and document a risk assessment to determine whether the violation poses a significant risk of financial, reputational or other harm to the individuals, considering such factors as to whom the disclosure was made, efficacy of steps to mitigate any harm, ability to determine extent of access, nature of the PHI, risk of re-identification of limited data set [OMB Memorandum M-07-16, pgs. 13-15, may provide helpful review of factors, See http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf]

9. Requirements regarding Timing, Content, Methods of Notification and Designated Recipients

164.404(a)-(b)
164.412

a. Timeliness 13402(c)-(d), (g)

i. Breach is treated as discovered on the first day that the CE or BA knew or, by exercising reasonable diligence would have known, of the violation; workforce should be adequately trained on importance of timely reporting

ii. Notice must be sent without unreasonable delay, but in no case later than 60 days after discovery of breach. It is unreasonable to delay notification within the 60 days if necessary information is available/compiled prior to that time. Information may be sent out in multiple mailings, as available, within the required time period.

iii. Law enforcement delay – if CE or BA receives official communication from law enforcement that notice or posting required hereunder would impede investigation

or threaten national security, notice shall be delayed as provided under 164.528(a)(2)

1. Oral notification must be documented, including the statement and the official's identity; may be for no longer than 30 days, unless followed with written notice
2. Written notification – delay for time period specified

b. Content - to extent possible, notice must include: 13402(f) *164.404(c)*

i. Brief description of event, including date of breach and date of discovery not including any PHI

ii. Description of types of unsecured PHI involved in breach

iii. Steps individual should take to protect self from potential harm from breach

iv. Brief description of what CE is doing to investigate, mitigate and protect from further harm or breach

v. Contact procedures for individuals to ask questions or seek information, including toll-free phone number, email address, web site or postal address

c. Methods of Notification 13402(e)(1) *164.404(d)*

i. Actual written notice to individual required

1. First class mail to last known address unless individual has consented to email notification
2. Notice to parent or representative for minor or individual lacking legal capacity
3. Notice to last known address of next of kin or personal representative for individuals known to be deceased

ii. If sufficient contact information is not available or communications are returned as undeliverable, CE must provide substitute notice as soon as reasonably possible

1. Must include required content set forth above
2. Not required for decedents
3. Must be reasonably calculated to reach the individuals
   - If fewer than 10 individuals – may be provided through alternate means, such as email or telephone [remaining sensitive to message content]
   - If 10 or more individuals – conspicuous posting for period of 90 or more days on home page of CE's web site [if hyperlinked from home page, link must be prominent and worded to convey nature and importance], or conspicuous notice in major print or broadcast media in geographic areas where the individuals likely reside, and toll-free phone number, active for at least 90 days must be included in notice

iii. Additional notice in urgent situations [i.e. threat of imminent misuse of PHI] may be made by other means than writing alone

iv. Notification to media: 13402(e)(2) *164.406*

1. Required if breach involves unsecured PHI of more than 500 residents of the state

- If breach involves PHI of 500 or more individuals, but not more than 500 residents of the state, media notice not required
- If breach occurs at BA serving multiple CEs and entities are unable to determine which entity's PHI is involved, CEs may consider having BA provide media notice

2. Content requirements are the same as for individual notice
3. If substitute notice is accomplished via media notice, the media notice must be reasonably calculated to reach individuals affected and meet all other requirements of the substitute notice as set forth above, including operation of the toll-free number
4. Provided to prominent media outlets serving the state
5. Supplements rather than displaces the individual notice
6. Subject to the same timeframe as individual notices

v. Notification to Secretary of HHS: 13402(e)(3) *164.408*

1. If breach involves PHI of 500 or more individuals (regardless of state residence), notice must be given to HHS concurrently with individual notices, subject to same timeframe
   - Mechanism for submission specified on HHS website
   - Lists of CEs submitting reports will be maintained on HHS website
2. If breach involves PHI of fewer than 500 individuals, CE must maintain a log or other documentation of breaches and submit information annually no later than 60 days after the end of each calendar year in manner described on HHS website
3. For calendar year 2009, submissions only required for breaches occurring on or after September 23, 2009
4. This does not supplant other reporting, documentation and retention requirements under the regulations

vi. Notification by a Business Associate (13402(b))– BA is required to notify all potentially affected CEs when it discovers a breach of unsecured PHI so that the CEs can make the notifications described above *164.410*

1. Breach is treated as discovered on the first day that the BA knew or, by exercising reasonable diligence any person other than the one committing the breach, who is an employee, officer or other agent, would have known, of the violation
   - Notice must be provided without unreasonable delay and in no case longer than 60 days of the discovery
   - Where BA is agent of CE, breach is imputed to CE – in order to permit CE to provide timely required notice, BAA should provide for a shorter timeframe for required BA notice
2. Content – to extent possible, notice must include:

- Identity of individuals whose PHI has been breached or is reasonably believed to have been breached
- Any other available information that the CE is required to include in its notice to the individual

3. Flexibility to address notice responsibilities within BAA as long as all requirements for notice are met

10. Administrative Requirements (13402(d))

164.414
164.530
160.534

a. Compliance with administrative requirements set forth in 164.530 – CE must comply with subsections (b), (d), (e), (g), (h), (i) and (j) of 164.530 with respect to breach notification provisions, including:

i. Development and documentation of policies and procedures

ii. Training of workforce members

iii. Application of sanctions for failure to comply with policies and procedures

iv. Provision for filing of complaints

v. Prohibition on intimidating or retaliatory acts

vi. Conforming amendments have been made to 164.530

b. CEs and BAs bear burden of demonstrating compliance with notice provisions, including determinations that notifications were not required

11. Preemption

160 Subpart B

a. Contrary state law is preempted by these provisions

i. Standard to be applied – whether CE could find it impossible to comply with both state and federal requirements or state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of the breach notification provisions

ii. Certain CE's exempted under Ohio's Security Breach Law – A state agency or an agency of a political subdivision that is a covered entity as defined in 45 CFR 160.103, as amended, is exempt from the security breach notice requirements of Section 1347.12 of the Ohio Revised Code.

INDEX

[MAIN HEADINGS in capitals; *definitions* in italics]

HIPAA Project Management Office

The Ohio Department of Job and Family Services

30 East Broad Street

Columbus Ohio, 43215

For additional information: http://hipaa.ohio.gov/