OHSU HIPAA Privacy Rule Glossary

The Privacy Rule contains many specialized terms and definitions. This glossary gives more information about how these terms are used in the Privacy Rule and what they mean.

Accounting of Disclosures – A disclosure is a release of information outside of OHSU. OHSU is required to keep a history of when and to whom protected health information (PHI) is disclosed if the disclosure occurs outside the scope of treatment, payment and health care operations, and is not authorized by the patient. A person has a right to receive an accounting of disclosures of PHI made by OHSU in the six years prior to the date of their request for an accounting, although OHSU is not required to begin tracking disclosures until April 14, 2003. Patients are entitled to one free accounting within any 12-month period. The accounting of disclosures lists:

- Date of disclosure;
- Name and, if known, address of the person or organization who received the information;
- Description of information disclosed;
- Brief statement of why the information was disclosed, or a copy of a written request for a disclosure.

Examples of a disclosure that OHSU would need to keep an accounting of would be:

- Releases to a coroner or medical examiner
- Releases for public health activities – such as HIV
- Releases required by law – such as abuse or neglect
- Releases for judicial proceedings – such as those required by a court order or subpoena

Authorization – As described within the Privacy Rule, an authorization is a written document signed by a patient that gives OHSU permission to use or disclose protected health information for purposes other than treatment, payment and health care operations. An authorization must contain:

- A specific description of the information to be used or disclosed
- The name or other specific identification of the person(s) making the request
- The name or other specific identification of the person(s) authorized to release the information
- The name or other specific identification of the person(s) authorized to receive the information
- The purpose of each use or disclosure
- An expiration date or event. For research, this may read “end of study” or “none.” If so, the authorization must clearly state that there is no expiration date.
- A statement of the individual’s right to revoke the authorization
- A statement that the information used or disclosed may be subject to re-disclosure
- A statement that treatment may not be conditioned on the signing of the authorization

A HIPAA authorization must be signed and dated by the individual or their representative and they must be given a copy.

Examples of disclosures for which authorizations are required include: Releasing the results of a pre-employment physical to an employer, or using protected health information for research activities.

Business Associate (BA) – A business associate is person or organization who uses PHI to perform a function, service, or activity for OHSU, or to help OHSU perform certain activities. A business associate may also create or store PHI on OHSU’s behalf. For those who perform these activities for OHSU, a business associate agreement (contract) must be in place by April, 2003. Business associate agreements describe what steps business associates must take to protect the privacy and security of PHI entrusted to them by OHSU. By definition, a business associate is NOT a member of OHSU’s workforce.

Examples of business associates are companies who perform claims processing or administration, accreditation,data analysis, billing, provide legal services, consulting, or accounting services.

Confidential Communication Restrictions – According to the Privacy Rule, OHSU must permit and accommodate reasonable requests for confidential communication of PHI. For example, a patient may request that any or all test results from OHSU be sent to an alternative address, such as a work address or a PO Box.

Data Use Agreement - A data use agreement is needed if health information is disclosed as a limited data set (see definition below.) The purpose of a data use agreement is to make sure that data is used in ways that are consistent with research, public health, or health care operations. It must limit who can use or receive the data, require the data recipient to agree not to re-identify the data or contact the subject of the information, and contain adequate assurances that the recipient will protect the data.

De-identified Information– De-identified information is health information that does not specifically identify an individual. Also, there is no reasonable basis to believe that the information alone *could* be used to identify an individual. In order to be considered de-identified, the following 18 elements must be removed: name; address; names of relatives; names of employers; birth date; telephone number; fax number; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; any vehicle or device serial number; web URL; Internet Protocol Address; Finger or voice prints; Photographic images (e.g. full facial photographs); and any other unique identifying number, characteristic, or code. Information may also be statistically de-identified. This is typically performed by an experienced statistician who analyzes the data and affirms that the risk is "very small" that a particular person could be identified from the information collected.

Designated Record Set (DRS) – The Designated Record Set are medical, dental, billing, and any other records used by OHSU to make decisions about patients. Patients have the right to inspect and copy their designated record set. If information in a patient's designated record set has been used or disclosed outside the scope of treatment, payment, and operations and the patient has not authorized this disclosure, the patient has a right to an accounting of it. If a patient requests a copy of their designated record set, OHSU has 30 days to satisfy this request. OHSU can impose a reasonable, cost-based fee for providing this documentation.

Some examples of the materials that could be included in the designated record set at OHSU would be the following: records centrally managed in HIS (paper, electronic), clinical site records, radiology records, dental records, billing records, off-site clinic records, etc.

Limited Data Set - A limited data set is information that is minimally identified by including a few selected identifiers. It may only contain: the subject's dates of admission and/or discharge, their date of death (if applicable), their date of birth (which can only be used as necessary), and the subject's five digit zip code or any other geographic subdivision (e.g., state, city, county.) The subject's street address cannot be included. Because a limited data set is not fully de-identified and could potentially be used to re-identify an individual, it is still subject to privacy protections. Therefore, if the data is going to be released to an outside party, a data use agreement, much like a business associate agreement, must be established between OHSU and the third party.

Marketing – According to the Privacy Rule, marketing is a communication about a product or service intended to encourage its purchase or use. Using PHI for marketing purposes requires an authorization from the patient, unless the communication is

A. A face-to-face communication made by a covered entity to an individual; or
B. A promotional gift of nominal value provided by OHSU.

Under the Privacy Rule, OHSU may also use and disclose PHI for the following activities without authorization:

A. Communications for the purpose of describing lists of providers in a provider or health plan network;
B. Communication for the purpose of describing lists of products or services provided by a OHSU or health benefit plan;
C. Communications tailored to the circumstances of a particular individual, made by a health care provider to an individual as part of the treatment of the individual, such as referrals, prescriptions, etc.
D. Communications for care management of the individual, or for the purpose of directing or recommending alternative treatments, therapies, providers, or care settings.

Minimum Necessary – When using, disclosing, or requesting protected health information OHSU must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This applies not only when we receive requests for PHI, but also to our requests for

information to other entities. OHSU must have policies and procedures in place which follow the minimum necessary standard.

For example, an employee at the call-center probably will not need all of the information contained in a patient's chart. Similarly, a health plan requesting patient information may not need access to the medical record information created under an individual's previous health plan.

Notice of Privacy Practices (NPP) – The notice of privacy practices describes how health information is used and disclosed and will describe the patient's rights regarding their health information. When the patient first arrives at OHSU, we must obtain the patient's acknowledgement that they have received a copy of this notice. If for some reason acknowledgement is not obtained, OHSU must document why. This notice will be available at all care-delivery sites as well as on the web.

Organized Health Care Arrangement (OHCA) – An Organized Health Care Arrangement is a legal definition described in the Privacy Rule. OHSU falls under this definition, and so is an OHCA. This means that within OHSU, different areas need to share protected health information about their patients, and that individuals who obtain services here expect that different areas share health information and are jointly managed.

The OHCA for OHSU includes, but is not limited to, the following: OHSU Hospital; Doernbecher Children's Hospital; all OHSU Ambulatory Clinics (including but not limited to: Casey Eye Institute, Dental Clinics, all Remote Clinics, IPCO Clinics, Employee Health and Student Health Services); Provost's Office; Human Resources; Vollum Institute; Center for Research on Occupational and Environmental Technology; Child Development and Rehabilitation Center; Neuro-Sciences Institute; School of Medicine; School of Dentistry; School of Nursing; OGI; the Primate Center; and OHSU Medical Group.

Psychotherapy Notes – Psychotherapy notes are notes recorded by a mental health professional which document or analyze the contents of conversation during a private counseling session or group, joint or family counseling session. In order to qualify as psychotherapy notes, these records must be separated from the rest of the individual's medical record. Psychotherapy notes do not include medication or prescription information, session start and stop times, types and frequency of treatment, results of clinical tests and summaries of diagnosis, functional status, treatment plans, symptoms, or prognosis and progress notes.

Protected Health Information (PHI) – The purpose of the HIPAA Privacy Rule is to protect and secure patients' PHI. PHI is information that relates to the past, present or future health of an individual, the provision of health care, or payment for the provision of health care to an individual, and which either identifies or could be used to identify a specific individual. Health information which includes any of the following identifiers is considered PHI, and so subject to the regulations contained in the privacy rule: name; address; names of relatives; names of employers; birth date; telephone number; fax number; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; any vehicle or devise serial number; web URL; Internet Protocol Address; Finger or voice prints; Photographic images; and any other unique identifying number, characteristic, or code.

Role-Based Access – OHSU must make a reasonable effort to assign individual access to PHI based on that person's role at OHSU. A person should only have access to the health information needed to fulfill their role here. Accordingly, individuals should have access to computer applications according to their position description and responsibilities.

For example, the access of a physician or nurse may be the entire health record. The access provided for a PAS specialist may be only scheduling and registration function. OHSU is required by the regulations to apply the minimum necessary concept by using the role-based model.

Training – OHSU must train all members of its workforce on how the HIPAA privacy standards will impact what they do at OHSU. All members of OHSU's workforce, including all full-, part-time and adjunct employees, faculty, staff, students, and volunteers, must be trained by April 14, 2003. The training is computer-based and is available by clicking here.

Treatment, Payment and Health Care Operations (TPO) - At OHSU, treatment, payment, and operations include the following activities:
Treatment – Provision, coordination, or management of health care and related services by one or more health care providers, including but not limited to

A. The coordination or management of health care by an OHSU health care provider with a third party;
B. Consultation between health care providers relating to a patient;
C. The referral of a patient for health care from one health care provider to another.

Payment - Activities undertaken by an OHSU health care provider to obtain reimbursement for the provision of health care, including but not limited to:

A. Determination of eligibility or coverage (including the coordination of benefits) and claim adjudication;
B. Risk adjustments;
C. Billing;
D. Claims management;
E. Collection activities;
F. Medical necessity review and/or justification of charges;
G. Utilizations review activities;
H. Disclosure to consumer reporting agencies relating to collection of premiums or reimbursement.

Health Care Operations - The necessary OHSU administrative, business, and education functions, including but not limited to:

A. Quality assessment and improvement activities
   Including:
   1. Outcomes evaluation and development of clinical guidelines (as long as such activities are not aimed at obtaining generalizable knowledge);
   2. 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;
   3. Related functions that do not include treatment.
B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, and health plan performance;
C. Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skill as health care providers;
D. Conducting training of non-health care professionals;
E. Accreditation activities;
F. Certification, licensing, or credentialing activities;
G. Insurance activities relating to the renewal or replacement of a contract for health insurance or health benefits;
H. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
I. OHSU business planning and development;
J. OHSU business management and administration activities Including, but not limited to:
   1. Customer service activities;
   2. Resolution of internal grievances;
   3. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity;
   4. Creating de-identified health information (45 CFR 164.514);
   5. Fundraising for the benefit of OHSU to the extent permitted without an authorization (45 CFR 164.514);
   6. Marketing to the extent permitted without an authorization (45 CFR 164.514)

Waiver of Authorization – For some research, obtaining authorization is impossible or simply not feasible. For instance, some epidemiological studies might access hundreds of thousands of records. In these cases, you may apply in writing for a waiver of authorization from the IRB. Once your application for a waiver has been sent to the IRB, it will be evaluated according to the following criteria:

The use or disclosure of PHI must involve no more than a minimal risk to the privacy of individuals. This is achieved by:

- Having an adequate plan to protect the PHI from improper use and disclosure

- Having a plan to destroy the PHI at the earliest opportunity consistent with the research,
- Having adequate written assurances from the investigator that the PHI will not be reused or disclosed to any other person or entity.

If there are health, research or legal justifications for not destroying the PHI, they will be taken into consideration by the IRB. The investigator must also show that the research would not be possible without a waiver or without access to the PHI in question. To obtain a waiver of authorization, a written request describing how the research meets the above criteria must be submitted to the IRB. The IRB will then review the request according to the standards of both the Common Rule and HIPAA and will approve or reject the request in writing.