Human Research Protection Program / Institutional Review Board

Standard Operating Procedure

2018 Common Rule

For Studies Initially Approved on or After January 21, 2019

Table of Contents

1 Health Insurance Portability and Accountability Act (HIPAA)

The *Health Insurance Portability and Accountability Act of 1996* (HIPAA) required the creation of a Privacy Rule for identifiable health information. While the primary impact of the Privacy Rule is on the routine provision of and billing for health care, the Rule also affects the conduct and oversight of research.

The Privacy Rule defines individually identifiable health information transmitted or maintained by a covered entity in any form (electronic, written or oral) as "protected health information" (PHI) and establishes the conditions under which investigators may access and use this information in the conduct of research.

Except as otherwise permitted, the Privacy Rule requires that a research subject "authorize" the use or disclosure of his/her PHI to be used in research. This authorization is distinct from the subject's consent to participate in research, which is required if the research is subject to the Common Rule, FDA regulations, and/or state laws that provide additional protection for research involving certain categories of health information (such as information derived from HIV/AIDS testing, genetic testing, and mental health records). When research consent is not required by regulation or law (e.g., for exempt research) or the requirement for research consent has been waived by an IRB, the requirements for authorization still apply unless an IRB or Privacy Board has determined that the criteria for a waiver of the authorization requirement are satisfied.

1.1 Definitions

Access. Access is the mechanism of obtaining or using information electronically, on paper, or other medium for the purpose of performing an official function.

Accounting of Disclosures. Information that describes a covered entity's disclosures of PHI other than for treatment, payment, and health care operations; disclosures made with Authorization; and certain other limited disclosures. For those categories of disclosures that need to be in the accounting, the accounting must include disclosures that have occurred during the 6 years (or a shorter time period at the request of the individual) prior to the date of the request for an accounting.

Authorization. An individual's written permission to allow a covered entity to use or disclose specified PHI for a particular purpose. Except as otherwise permitted by the Privacy Rule, a covered entity may not use or disclose PHI for research purposes without a valid Authorization that includes all of the required elements under the Privacy Rule.

Covered entity. A health plan, a health care clearinghouse, or a health care provider who or that transmits health information in electronic form in connection with a transaction for which DHHS has adopted a standard.

Data Use Agreement. An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and disclosed and how it will be protected.

De-identified. Data are considered de-identified under HIPAA when they do not identify an individual, and there is no reasonable basis to believe that the data can be used to identify an individual. The Privacy Rule defines two methods for de-identifying PHI: (1) when the PHI is stripped of all 18 HIPAA-defined identifying

elements and the covered entity 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 (Safe Harbor method); or (2) when an appropriate expert 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 (Expert Determination method).

Designated Record Set. A group of records maintained by or for a covered entity that includes (1) medical and billing records about individuals maintained by or for a covered health care provider; (2) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the covered entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

Disclosure. The release, transfer, provision of access to, or divulging in any manner, of information outside the entity holding the information.

Genetic Information. Genetic information means, with respect to an individual, information about:
(i) The individual's genetic tests; (ii) The genetic tests of family members of the individual;
(iii) The manifestation of a disease or disorder in family members of such individual; or iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

Genetic information concerning an individual or family member of an individual includes the genetic information of: (i) A fetus carried by the individual or family member who is a pregnant woman; and (ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology. Genetic information excludes information about the sex or age of any individual.

Genetic services. A genetic test; genetic counseling (including obtaining, interpreting, or assessing genetic information); or genetic education.

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Health Information. Health Information means any information, including genetic information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) 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.

Individually Identifiable Health Information. Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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 (a) that identifies the individual; or (b)

with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Limited Data Set. Refers to data sets that exclude 16 categories of direct identifiers that are specified in the Privacy Rule. Limited Data Sets may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, only if the covered entity obtains satisfactory assurances in the form of a Data Use Agreement. Limited Data Sets are not de-identified information under the Privacy Rule.

Minimum Necessary. The least PHI reasonably necessary to accomplish the intended purpose of the use, disclosure, or request. Unless an exception applies, this standard applies to a covered entity when using or disclosing PHI or when requesting PHI from another covered entity. A covered entity that is using or disclosing PHI for research without Authorization must make reasonable efforts to limit PHI to the minimum necessary. A covered entity may rely, if reasonable under the circumstances, on documentation of IRB or Privacy Board approval or other appropriate representations and documentation under section 164.512(i) as establishing that the request for PHI for the research meets the minimum necessary requirements.

Privacy Board. A board that is established to review and approve requests for waivers or alterations of Authorization in connection with a use or disclosure of PHI as an alternative to obtaining such waivers or alterations from an IRB. A Privacy Board consists of members with varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on an individual's privacy rights and related interests. The board must include at least one member who is not affiliated with the covered entity, is not affiliated with any entity conducting or sponsoring the research, and is not related to any person who is affiliated with any such entities. A Privacy Board cannot have any member participating in a review of any project in which the member has a conflict of interest.

Protected Health Information. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); in employment records held by a covered entity in its role as employer; and regarding a person who has been deceased for more than 50 years.

Psychotherapy Notes. Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Research. A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research.

Use. With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the covered entity or health care component (for hybrid entities) that maintains such information.

Waiver or Alteration of Authorization. The documentation that the covered entity obtains from a researcher or an IRB or a Privacy Board that states that the IRB or Privacy Board has waived or altered the Privacy Rule's requirement that an individual must authorize a covered entity to use or disclose the individual's PHI for research purposes.

Workforce. Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of the covered entity, whether or not they are paid by the covered entity.

1.2 The IRB's Role under the Privacy Rule

Under the Privacy Rule, IRBs have authority to consider, and act upon, requests for a partial or complete waiver or alteration of the Privacy Rule's Authorization requirement for uses and disclosures of PHI for research. Although the Common Rule and FDA regulations include protections to help ensure the privacy of subjects and the confidentiality of information (as applicable, to research activities that are regulated under those sets of regulations), the Privacy Rule supplements these protections where HIPAA is applicable, by requiring covered entities to implement specific measures to safeguard the privacy of PHI. If certain conditions are met, an IRB may grant a waiver or an alteration of the Authorization requirement for research uses or disclosures of PHI.

MaineHealth's IRB and, when mutually agreed, the external IRBs it relies upon, fulfill the functions of a Privacy Board for human subject research.

The Privacy Rule does not change the composition of an IRB. When acting upon a request to waive or alter the Authorization requirement, an IRB must follow the procedural requirements of the Common Rule and FDA regulations, if applicable, including using either the normal review procedures (review by the convened IRB) or, as appropriate, the expedited review procedures.

When a request for a waiver or an alteration of the Authorization requirement is considered by the convened IRB, a majority of the IRB members must be present at the meeting, including at least one member whose primary concerns are in nonscientific areas. In order for an approval of a waiver or an alteration of the Privacy Rule's Authorization requirement to be effective, it must be approved by a majority of the IRB members present at the convened meeting. If a member of the IRB has a conflicting interest with respect to the PHI use and disclosure for which a waiver or an alteration approval is being sought, that member may not participate in the review. Expedited review of a request for a waiver or an alteration of the Authorization requirement is permitted if the research study qualifies for expedited review under DHHS requirements. A modification to a previously approved research protocol, which only involves the addition of an Authorization for the use or disclosure of PHI to the IRB-approved informed consent, may be reviewed by the IRB through an expedited review procedure, because this type of modification may be considered to be no more than a minor change to research. If expedited review procedures are appropriate for acting on the request, the review may be carried out by the IRB Chair or by one or more experienced reviewers designated by the Chair from among the IRB

members. A member with a conflicting interest may not participate in an expedited review. If an IRB uses expedited review procedures, it must adopt methods for keeping all its members advised of all requests for waivers or alterations of the Authorization requirement as well as those requests that have been granted under an expedited review procedure.

IRB documentation of approval of a waiver or alteration of the authorization requirement includes:

1. The identity of the approving IRB;
2. The date on which the waiver or alteration was approved;
3. A statement that the IRB has determined that the alteration or waiver or authorization, in whole or in part, satisfies the three criteria in the Rule;
4. A brief description of the PHI for which use or access has been determined to be necessary by the IRB;
5. A statement that the waiver or alteration was reviewed and approved under either normal or expedited review procedures; and
6. The signature of the IRB Chair or other member, as designated by the Chair, of the IRB, as applicable.

MaineHealth will not release PHI to investigators or other third parties without individual authorization or proper documentation of an IRB or Privacy Board approval of a waiver or alteration of the requirement.

1.3 Authorization

Except as otherwise permitted, the Privacy Rule requires that a research subject "authorize" the use or disclosure of his/her PHI to be used in research. This authorization is distinct from the subject's consent to participate in research, which is required for research to which the Common Rule, FDA regulations, and/or state laws regarding certain categories of health information apply (although certain research that is subject to the Privacy Rule may be exempt from Common Rule requirements). Just as a valid consent under Common Rule and FDA regulations must meet certain requirements, a valid authorization must be written in plain language and contain certain statements and core elements [45 CFR 164.508.6(c)]. At MaineHealth, the HIPAA authorization is documented within the consent document, and is reviewed along with all other materials submitted for IRB review and approval.

Once executed, a signed copy must be provided to the individual providing authorization. Signed authorizations must be retained by the covered entity for 6 years from the date of creation or the date it was last in effect, whichever is later.

A research subject has the right to revoke their authorization at any time. See Section 27.12 for more information regarding an individual's right to revoke, procedures, and exceptions.

When an Authorization permits disclosure of PHI to a person or organization that is not a covered entity (such as a sponsor or funding source), the Privacy Rule does not continue to protect the PHI disclosed to such entity. However, other federal and state laws and agreements between the covered entity and recipient such as a Business Associate Agreement (BAA) or Confidentiality Agreement may establish continuing protections for

the disclosed information. Under the Common rule or FDA regulations, an IRB may impose further restrictions on the use or disclosure of research information to protect subjects.

Authorization Core Elements:

1. A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner;
2. The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure;
3. The names or other specific identification of the person or persons (or class of persons) to whom the covered entity may make the requested use or disclosure;
4. A description of each purpose of the requested use or disclosure;
5. Authorization expiration date or expiration event that relates to the individual or to the purpose of the use or disclosure (A statement that there is "no expiration date or event" or that authorization expires at the "end of the research study" or "unless and until revoked" by the individual are permissible for research, including authorizations for future research; and
6. The signature of the individual and date. If the individual's legally authorized representative signs the Authorization, a description of the representative's authority to act for the individual must also be provided.

Authorization Required Statements:

1. A statement of the individual's right to revoke his/her Authorization and how to do so, and, if applicable, the exceptions to the right to revoke his/her Authorization or reference to the corresponding section of the covered entity's notice of privacy practices;
2. Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on Authorization (if such conditioning is permitted under the Privacy Rule), including research-related treatment and consequences of refusing to sign the Authorization; and
3. A statement of the potential risk that PHI will be re-disclosed by the recipient. This may be a general statement that the Privacy Rule may no longer protect health information disclosed to the recipient.

1.4 Waiver or Alteration of the Authorization Requirement

Obtaining signed authorization to access and use of PHI for research is not always feasible. The Privacy Rule contains criteria for waiver or alterations of authorization. If a covered entity has used or disclosed PHI for research pursuant to a waiver or alteration of authorization, documentation of the approval of the waiver or alteration must be retained for 6 years from the date of its creation or the date it was last in effect, whichever is later. This is in addition to any other documentation requirements that might apply.

For research uses and disclosures of PHI, an IRB or Privacy Board may approve a waiver or an alteration of the authorization requirement in whole or in part. A complete waiver occurs when the IRB or Privacy Board determines that no authorization will be required for a covered entity to use and disclose the PHI

contemplated to be used or disclosed for that particular research project. A partial waiver of authorization occurs when the IRB or Privacy Board determines that a covered entity does not need authorization for all PHI uses and disclosures for some defined group of research purposes, such as accessing PHI for research recruitment purposes. An IRB or Privacy Board may also approve a request that removes some, but not all, required elements or statements of an authorization (an alteration).

In order for an IRB or Privacy Board to waive or alter authorization, the Privacy Rule (45 CFR 164.512(i)(2)(ii)) requires the IRB or Privacy Board to determine the following:

1. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
    a. An adequate plan to protect health information identifiers from improper use and disclosure;
    b. An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    c. Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under the Privacy Rule;
2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably be conducted without access to and use of the PHI.

The Privacy Rule allows institutions to rely on a waiver or an alteration of Authorization obtained from a single IRB or Privacy Board to be used to obtain or release PHI in connection with a multi-site project.

1.5 Activities Preparatory to Research

Under the preparatory to research provision of the Privacy Rule, a covered entity may permit a research to use PHI for purposes preparatory to research such as assessing the feasibility of conducting a research project, developing a grant application or protocol, or identifying potential subjects.

The covered entity must obtain from the investigator representations, either in writing or orally, that (1) the use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research, (2) that the investigator will not remove any PHI from the covered entity (e.g., physically taken out of a facility, or downloaded and retained on the investigator's device) in the course of the review, and (3) the PHI for which access is sought is necessary for the research purpose. [45 CFR 164.512(i)(1)(ii)]

Federal guidance has drawn a distinction between activities that may be undertaken by a researcher who is a member of the covered entity's workforce, e.g., an employee of the covered entity, and a researcher who is not part of the covered entity's workforce. This guidance indicates that researchers may use PHI under the preparatory to research provision to *identify* potential study participants, so long as no PHI is removed from the covered entity and the remaining two representations set forth above can be made. However, the guidance also indicates that researchers may not use PHI obtained pursuant to the "preparatory to research"

provision to *contact* potential study subjects unless (i) the researcher is a member of the covered entity's workforce, or (ii) the researcher enters into a BAA with the covered entity. Therefore, if the researcher is not a workforce member or business associate of the covered entity, then the researcher may contact potential subjects only pursuant to a partial waiver of authorization from the cognizant IRB or privacy board, or pursuant to the Authorization of the subject.

MaineHealth further requires that first contact with a patient for recruitment into a study must always be via a MaineHealth individual who has a treatment relationship with that patient. These details, along with approved recruitment tools (e.g., script or flyer etc.) to be used by the individual with the treatment relationship, must be provided in the IRB submission.

1.6 Research Using Decedent's Information

The HIPAA Privacy Rule protects the individually identifiable health information about a decedent for 50 years following the date of death of the individual. When a researcher seeks to use PHI from decedents for a research protocol, the researcher must (1) obtain authorization from the personal representative of the decedent (i.e., the person under applicable law with authority to act on behalf of the decedent or the decedent's estate), (2) obtain a waiver of the requirement to obtain authorization from an IRB or Privacy Board, or (3) attest to the covered entity holding the PHI that the use or disclosure is solely for research on the PHI of decedents, that the PHI being sought is necessary for the research, and, if requested by the covered entity, provide documentation of the death of the individuals about whom information is being sought.

At MaineHealth, the attestation option referenced above is accomplished by the investigator submitting a Research Use of Decedents' PHI Attestation to the Office of Research Compliance.

1.7 Storage and Use of PHI for Future Research

The Privacy Rule recognizes the creation of a research database or a specimen repository to be a research activity if the data/specimens to be stored contain PHI. When researchers establish a database or repository containing PHI for the purposes of future research, or intend to maintain the PHI following completion of a primary study for potential future research use, individual authorization for the **storage** of PHI for such future research must be sought unless the IRB has determined that the criteria for a waiver of the authorization requirement are satisfied. See Section 27.4 of this policy manual for a discussion of waivers of authorization.

An authorization for use and/or disclosure of the stored PHI for **future research** must describe the future research uses and/or disclosures in sufficient detail to allow the potential subject to make an informed decision. The Rule does not require that an authorization describe each specific future study if the particular studies to be conducted are not yet determined. Instead, the authorization must adequately describe future purposes such that it would be reasonable for the subject to expect that their PHI could be used or disclosed for such research. When developing the description of potential future research uses, the investigator should be cognizant of uses of information/specimens that the community may consider particularly sensitive, such as genetics, mental health, studies of origin, and use of tissues that may have cultural significance, including whether any state laws may impose additional consent requirements with respect to any of these sensitive categories of information.

The authorization for future research can be a stand-alone document or may be incorporated into the authorization for the establishment of the database or repository or for the primary study, unless the research involves the use or disclosure of psychotherapy notes. Authorizations for the use or disclosure of psychotherapy notes can only be combined with another authorization for a use or disclosure of psychotherapy notes.

If the authorization for future research is combined with the authorization for the primary study, the authorization must clearly differentiate between the authorization for the primary study and the authorization for the unspecified future research activities, and allow the subject to opt-in to the future research. Opt-outs for future research are not permitted under the Privacy Rule because an opt-out process does not provide individuals with a clear ability to authorize the use of their information/specimens for future research, and may be viewed as coercive.

It is important to note that securing a HIPAA authorization for unspecified future research activities may not, by itself, satisfy all applicable legal consent requirements. The Common Rule, FDA regulations, and state laws also must be considered, as applicable, in evaluating whether the information (including PHI) or identifiable biospecimens may be used for future research projects.

1.8 Corollary and Sub-studies

Consistent with the discussion above relating to future uses of research databases or repositories, the Privacy Rule mandates that subject participation in corollary or sub-studies not essential to the primary aims of the research, such as when PHI form an interventional clinical trial is used to create or to contribute to a central research repository, must be on a voluntary, "opt-in" basis. This is particularly important when the primary research offers a potential direct benefit to the research subject, such as treatment, that might compel the potential subject to agree to an ancillary study, even if the subject would prefer not to do so.

HIPAA reinforces this ethical principle by explicitly stating that authorization for "unconditioned" activities, for which there is no associated treatment, benefit or other effect on the individual subject associated with participation, cannot be required. The published preamble to HIPAA Omnibus clarifies the basis for this position, and the requirement that authorization for unconditioned activities involve a clear opt-in mechanism, stating:

> *"This limitation on certain compound authorizations was intended to help ensure that individuals understand that they may decline the activity described in the unconditioned authorization yet still receive treatment or other benefits or services by agreeing to the conditioned authorization." and "an opt out option does not provide individuals with a clear ability to authorize the optional research activity, and may be viewed as coercive by individuals."*

As with authorization for future research (which is one form of "unconditioned activity"), it is acceptable to combine in a single document the authorization for a conditioned activity, such as a clinical trial, with authorization for other forms of unconditioned activities such as a corollary or sub-study that does not directly benefit or effect the individual participant, **provided that**:

1. The authorization clearly differentiates between the conditioned and unconditioned research activities;
2. The authorization clearly allows the individual the option to opt in to the unconditioned research activities; and
3. Sufficient information is provided for the individual to be able to make an informed choice about both the conditioned and unconditioned activities.

Separate authorization must be obtained for research activity that involves the use and disclosure of psychotherapy notes. For example, authorization for the use and disclosure of psychotherapy notes for a clinical trial cannot be combined with an authorization for the use and disclosure of those psychotherapy notes for a corollary research activity.

1.9 De-identification of PHI under the Privacy Rule

Covered entities may use or disclose health information that is de-identified without restriction under the Privacy Rule, because information that has been de-identified consistent with the Privacy Rule requirements is not considered individually identifiable health information. The "Safe Harbor" method permits a covered entity to de-identify data by removing all 18 data elements specified in the Privacy Rule that could be used to identify the individual who is the subject of the information or the individual's relatives, employers, or household members. To satisfy the Safe Harbor method of de-identification, the covered entity also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify individuals. Under this method, the identifiers of the individual or his or her relatives, employers, or household members that must be removed are the following:

1. Names;
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
    a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people;
    b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Facsimile numbers;
6. Electronic mail addresses;

7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web universal resource locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including fingerprints and voiceprints;
17. Full-face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

Alternatively, a qualified statistician may certify that the risk is very small that the health information could be used, alone or in combination with other reasonably available information, to identify individuals. The qualified statistician must document the methods and results of the analysis that justify such a determination. This analysis must be retained by the covered entity for 6 years from the date of its creation or when it was last acted on, whichever is later.

The Privacy Rule permits a covered entity to assign to, and retain with, the de-identified health information, a code or other means of record re-identification if that code **is not** derived from or related to the information about the individual and is not otherwise capable of being translated to identify the individual. The covered entity may not use or disclose the code or other means of record identification for any other purpose and may not disclose its method of re-identifying the information.

NOTE: Data that are considered de-identified under HIPAA may still be considered human subject data under the Common Rule and may require IRB review and approval. Removal of HIPAA-identifying elements does not necessarily mean that the identity of the subject is not or may not readily be ascertained by the investigator or associated with the information and thus be considered identifiable private information under the Common Rule. The reverse can also be true (and, in practice, is more likely to occur): information may not be "identifiable" under the Common Rule but, because it contains certain HIPAA identifiers, it is considered identifiable under HIPAA.

1.10 Limited Data Sets and Data Use Agreements

Limited data sets are data sets stripped of certain direct identifiers. Limited data sets may be used or disclosed only for public health, research, or health care operations purposes. Because limited data sets may contain identifiable information, they are still PHI and as such are not considered de-identified under the

Privacy Rule. Unlike de-identified data, Protected Health Information in limited data sets may include: addresses other than street name or street address or post office boxes, all elements of dates (such as admission and discharge dates) and unique codes or identifiers not listed as direct identifiers. The following direct identifiers must be removed for PHI to qualify as a limited data set:

1. Names;
2. Postal address information, other than town or city, state, and ZIP code;
3. Telephone numbers;
4. Fax numbers;
5. Email addresses;
6. Social Security numbers;
7. Medical Record numbers;
8. Health Plan Beneficiary numbers;
9. Account numbers;
10. Certificate or license numbers;
11. Vehicle identifiers and license plate numbers;
12. Device identifiers and serial numbers;
13. URLs;
14. IP addresses;
15. Biometric identifiers; and
16. Full-face photographs and any comparable images.

Before disclosing a limited data set, a covered entity must enter into a Data Use Agreement (DUA) with the recipient, even when the recipient is a member of its workforce. The DUA establishes the parameters around the proposed uses and disclosures of the data, who is permitted to have access to the data, and stipulates that no other use or disclosure will be made other than as permitted by the DUA or as otherwise required by law, no attempt will be made to identify or contact individuals whose data are included in the limited data set, that appropriate safeguards are in place to protect the data from unauthorized use or disclosure, that any agents, including subcontractors, to whom the recipient provides the LDS will agree to the same restrictions and conditions that apply to the recipient, and that the recipient will report any uses or disclosures of the information that they become aware of that are not in keeping with the terms of the DUA. Data Use Agreements for the purposes of research are available through Grants and Contracts.

1.11 Research Subject Access to PHI

With few exceptions, the Privacy Rule guarantees individuals access to their medical records and other types of health information. One exception is during a clinical trial, when the subject's right of access can be

suspended while the research is in progress. The subject must have been notified of and agreed to the temporary denial of access when providing consent and authorization. Any such notice must also inform the individual that the right to access will be restored upon conclusion of the clinical trial. Language accommodating this exclusion is included in the applicable MaineHealth authorization template.

1.12 Revoking Authorization

The Privacy Rule establishes the right for an individual to revoke their authorization for uses and disclosures of PHI for research, in writing, at any time, except to the extent that the covered entity has taken action in reliance on the authorization. [45 CFR 164.508(b)(5)] However, individuals providing authorization should be made aware that revoking authorization does not mean that the individual's PHI may no longer be used in the research or be used or disclosed for other purposes.

At MaineHealth, individuals may revoke authorization by requesting the investigator stop collecting their data. This request may be made by phone, but must also be accompanied by a written request. The investigator will report all subject withdrawals at the time of continuing review. However if the subject withdraws due to an unresolved complaint, or due to an unanticipated problem involving risk to that subject, ORC should be notified as soon as possible in accordance with these SOPs.

A covered entity may continue to use and disclose PHI that was obtained **before** the individual revoked authorization to the extent that the entity has taken action in reliance on the authorization. When the research is being conducted by the covered entity, the covered entity is permitted to continue using or disclosing the **already obtained** PHI to the extent necessary to maintain the integrity of the research (e.g., to account for a subject's withdrawal from a study, to report adverse events, or to conduct an investigation of misconduct). A covered entity may also continue to use the PHI for other activities that are permitted under the Rule without authorization (e.g., health care operations such as QA/QI). Additionally, revoking an authorization does not prevent the continued use or disclosure of PHI by a non-covered entity that had **already received** it pursuant to the authorization.

1.13 Accounting of Disclosures

The Privacy Rule generally grants individuals the right to a written "Accounting of Disclosures" of their Protected Health Information made by a covered entity without the individual's authorization in the six years prior to their request for an Accounting. A covered entity must therefore keep records of such PHI disclosures for 6 years.

It is important to understand the difference between a use and a disclosure of PHI. In general, the use of PHI means use of that information within the covered entity. A disclosure of PHI means "the release, transfer, provision of access to, or divulging in any manner of information outside of the entity holding the information." The Privacy Rule restricts both uses and disclosures of PHI, but it requires an accounting only for certain PHI disclosures.

Generally, an Accounting of Disclosures is required for:

1. Routinely Permitted Disclosures (e.g., under public health authority, to regulatory agencies, to persons with FDA-related responsibilities) with limited exceptions (e.g., law enforcement, national security, etc.);
2. Disclosures made pursuant to:
    a. Waiver of Authorization;
    b. Research on Decedents' Information; or
    c. Reviews Preparatory to Research.

An accounting is not needed when the PHI disclosure is made:

1. For treatment, payment, or health care operations;
2. Under an Authorization for the disclosure.;
3. To an individual about himself or herself; or
4. As part of a limited data set under a data use agreement.

The Privacy Rule allows three methods for accounting for research-related disclosures that are made without the individual's Authorization or other than a limited data set: (1) A standard approach, (2) a multiple-disclosures approach, and (3) an alternative for disclosures involving 50 or more individuals. Whatever approach is selected, the accounting is made in writing and provided to the requesting individual. Accounting reports to individuals may include results from more than one accounting method.