The HIPAA Privacy Rule and Public Health Laboratories

Guidance

Prepared for the Association of Public Health Laboratories

James G. Hodge, Jr., J.D., LL.M.

Adjunct Professor of Law, Georgetown University Law Center
Assistant Scientist, the Johns Hopkins Bloomberg School of Public Health
Deputy Director, Center for Law and the Public’s Health
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY** ......................................................................................................... 4

**INTRODUCTION** ........................................................................................................................ 6

The Need for National Health Information Privacy Protections ................................. 6
Impact of the Privacy Rule on Public Health................................................................. 7

**OVERVIEW OF THE PRIVACY RULE** ............................................................................... 9

Who is Covered? .................................................................................................................. 9
Who is Not Covered? ....................................................................................................... 10
What Information is Protected? ......................................................................................... 10

*Text Box – Comprehensive Set of Individual Identifiers Under the Privacy Rule*

What Information is Not Protected? .............................................................................. 11
What Does the Rule Require? ............................................................................................ 12
What Are the Provisions Regarding Uses and Disclosures? ............................................ 13
  Required Disclosures ............................................................................................. 13
  Disclosures for Treatment, Payment, and Health Care Operations ....................... 13

*Text Box - Standard Transactions Under HIPAA*

Authorized Disclosures ........................................................................................................ 14
Permissible Disclosures without Authorization ......................................................... 14

Does the Rule Preempt State or Local Laws? ................................................................. 15

**IMPACT OF THE PRIVACY RULE ON PUBLIC HEALTH LABORATORIES** .......... 16

External Impact – The Public Health Provisions............................................................ 16
  What is a Public Health Authority? .................................................................................. 16
  Permitted Disclosures for Public Health........................................................................ 17
  Other Permissible Disclosures Without Authorization................................................. 17
  Other Requirements for Covered Entities ....................................................................... 18
  The “Minimum Necessary” Standard ............................................................................ 18

Internal Impact – Public Health Performing Covered Functions...................................... 19
  Do Public Health Laboratories Perform Covered Functions? ....................................... 19
  Public Health Laboratories As Health Care Providers ................................................. 20

Public Health Laboratories and Electronic Transmissions .................................................. 21
EXECUTIVE SUMMARY

On April 14, 2003, most “covered entities” (large health plans, health care clearinghouses, and health care providers) and their business associates must comply with the new HIPAA Privacy Rule (“Rule”).

Together with new security standards issued by the Department of Health and Human Services (HHS), the Privacy Rule provides the first national standards for protecting the privacy and security of individually identifiable health information (i.e. “protected health information,” or “PHI”) in public and private sectors.

Though the Rule is focused on protecting individual privacy interests in health data, HHS acknowledges the communal need to share PHI for important health objectives like public health and health research. Public health laboratories (and their larger public health agencies) need identifiable health data to accomplish their public health and clinical goals. These laboratories conduct tests on patient biological samples to determine whether an individual may have a particular disease or condition, or may have been exposed to environmental contaminants. Test results are typically reported in an identifiable format to the patient’s requesting physician, public health authorities, and sometimes to the patient. These data may constitute PHI as defined by the Rule.

The impact of the Privacy Rule on public health authorities and laboratories can be examined from external (what external barriers limit laboratories’ access to and use of PHI?) and internal (what internal functions of a lab are covered under the Rule?) perspectives.

Among the external impacts of the Privacy Rule on public health laboratory practices are the following:

- While the Rule allows for the unauthorized disclosure of PHI by covered entities to public health authorities for public health purposes or to provide health care services, disclosures of PHI to public health labs for other purposes (e.g., health research) are limited.
- Subsequent disclosures of most PHI by a public health lab may be subject to similar limitations as those faced by covered entities. This includes ensuring that disclosures are limited to the minimal amount of information necessary.
- Although a covered entity providing PHI to a public health lab for treatment purposes does not have to account for these disclosures, other disclosures (for public health purposes) may have to be accounted for by the covered entity. Some covered entities suggest that the accounting requirement may stop them from sharing some health data with others.

Internally, the Privacy Rule can affect public health labs in the same ways it affects covered entities.
• When a public health lab provides health care services, like diagnostic tests, its activities are viewed as covered under the Rule if it conducts any of a series of health care transactions electronically.
• Correspondingly, the lab must provide the same privacy protections for PHI created or used during these activities as most other covered entities.
• Because they also perform public health functions, public health labs (or their parent agencies) may choose to classify themselves as hybrid entities under the Rule. This allows the labs to designate only certain activities as “covered” under the Rule.
• Specific exemptions regarding individual access under the Rule defer to the access/disclosure requirements under the Clinical Laboratory Amendments (CLIA) or relevant state law.
• State public health labs also serving as forensic labs that perform autopsies or other procedures may produce health data related to deceased persons. This data may constitute PHI since the Rule’s coverage extends to deceased persons (subject to several exceptions).
INTRODUCTION

Through Congressional authority via the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) has created the Privacy Rule (also known as Standards for Privacy of Individually Identifiable Health Information)\(^1\) and companion security protections standards (also known as HIPAA Security Standards Final Rule).\(^2\)

On April 14, 2003, most “covered entities” (including large health plans, health care clearinghouses, and health care providers that transmit certain administrative and financial transactions electronically), and their “business associates” (e.g., claims processors, billing managers, data analyzers, and others), must comply with the Rule. HHS’ Office for Civil Rights (OCR) has oversight and enforcement responsibilities for the Rule. The U.S. Department of Justice is responsible for enforcing criminal penalties for some violations.

Together, these regulations provide for the first time national standards for protecting the privacy and security of individually identifiable health information (i.e. “protected health information,” or “PHI”) in many public and private sectors. The Privacy Rule requires a range of personal privacy protections and measures, including provisions regarding:

- Notice to individuals about their privacy rights and how their PHI is used or disclosed;
- Individual rights to inspect and request corrections or amendments to PHI;
- Disclosure limitations for non-health care transactions;
- New privacy criteria to assess in reviewing health research projects;
- Security protections for PHI; and
- Implementation of internal privacy procedures.

The Need for National Health Information Privacy Protections

National privacy and security safeguards are needed because actual and perceived privacy risks underlying the increased proliferation of (and access to) identifiable health data as medical records shift from paper to electronic formats within the national health information infrastructure. People are concerned about how their sensitive health data are handled and exchanged.

Although protecting individual privacy is a long-standing tradition among health care providers and public health practitioners, existing legal protections at the federal, tribal, state, and local levels are generally viewed as fragmented, inconsistent, and inadequate. A patchwork of federal and state laws typically provides narrow privacy protections for selected types of health data or information held by certain entities.\(^5\)

HHS addresses these privacy concerns by creating new privacy and security standards that set a national floor of basic protections and “balance the needs of the individual with the needs of society.”\(^6\) In addition to the importance of protecting individual privacy rights, HHS acknowledges the communal need to share PHI to accomplish important health objectives (e.g.,
Public health agencies and laboratories at the federal, tribal, state, and local levels of government need access to identifiable health data to protect the health of the public. Public health practice and research—including traditional public health activities such as public health surveillance, outbreak investigations, direct health services, and epidemiological research—require the acquisition, use, and disclosure of PHI. Identifiable health data are essential to help authorities monitor and respond to the incidence, patterns, and trends of injury and disease among populations.

Public health laboratories produce identifiable health information that the public health community needs. State or local public health laboratories conduct tests on patient’s biological samples to determine whether the individual may have a particular disease or condition, or may have been exposed to environmental contaminants. These test results, reported with identifiers to the patient’s requesting physician, public health authorities, and sometimes to the patient as well, are the sort of identifiable health information that the Rule pertains.

Public health laboratories understand the need to protect individual privacy to respect individual dignity and maintain the quality and integrity of health data. They realize that people and their physicians may avoid public health laboratory services if they feel that their health information is handled irresponsibly.

Impact of the Privacy Rule on Public Health

While the Privacy Rule is primarily directed at covered entities, the Rule impacts public health authorities, including laboratories. In an effort to minimize the impact of this Rule on public health, the Rule explicitly permits PHI to be shared with public health authorities for public health purposes, and with researchers for research activities (under a specific exception).

The affects of the Rule on public health authorities and laboratories can be examined from external and internal perspectives. What are external barriers, real or perceived, that may confront and limit public health laboratories’ access to and use of protected health information? Additionally, what are the internal, operational barriers that the Rule may impose on public health labs?

To the extent the Privacy Rule regulates the use and disclosure of PHI by covered entities, questions regarding its external impacts on public health laboratories include:

- Does the Privacy Rule limit the disclosure of PHI by covered entities to public health labs or their contractors/partners for health care or public health purposes?
- Does the Rule limit subsequent disclosures of PHI by public health labs?
- Does a covered entity providing PHI to a public health lab have to account for these disclosures?
Internally, the Privacy Rule affects public health labs in similar ways as it does covered entities when labs assimilate the activities of health care providers. A local public health lab, for example, that provides direct testing services to patients of a local physician may be defined under the Rule as a “health care provider.” Questions regarding the internal impact of the Rule on public health laboratories include:

- When does a public health lab perform “covered functions” under the Rule?
- Does a public health authority that performs covered functions have to meet all of the requirements of the Rule? Specifically, what about the Rule’s individual access provisions?
- What if one part or division of public health lab is subject to the Rule – is the entire agency required to comply?

This brief Guidance addresses these and some other questions and issues concerning the effect of the Privacy Rule on public health laboratories. It begins with a brief overview of the Privacy Rule to answer some basic questions, including:

- Who is (not) covered?
- What information does the Rule apply (or not apply) to?
- What does the Rule require?
- What are the provisions concerning uses and disclosures; and
- Does the Rule preempt state or local laws?

The document then focuses exclusively on the effect of the Privacy Rule on public health laboratories by discussing external and internal impacts of the Rule.

Additional guidance on the impact of the Rule on public health agencies is available through the CDC’s forthcoming HIPAA Guidance document. This guidance will be published in a summary format as a Report and Recommendation in the Morbidity and Mortality Weekly Reporter. A more comprehensive version is also to be made available via electronic publication on CDC’s website.

Please refer to Appendix A, A Glossary of Terms Associated with HIPAA’s Privacy and Security Rules, for definitions of many of the specific terms (e.g., protected health information, covered entity, public health authority, . . .) used in this document.
OVERVIEW OF THE PRIVACY RULE

On April 14, 2001, President Bush approved the Privacy Rule\textsuperscript{11} pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).\textsuperscript{12} The Rule’s provisions represent the first systematic national privacy protections of health information.

Through HIPAA, Congress originally imposed a deadline of August 21, 1999 to pass national health information privacy legislation. The Act further authorized the Secretary of the Department of Health and Human Services (HHS) to issue privacy regulations if Congress failed to act within its self-imposed deadline.

Initial publication of HHS’ proposed Rule in November, 1999 garnered thousands of public comments. Final production was delayed until December, 2000. On April 14, 2001, the Rule was accepted subject to interpretive guidelines by HHS’ Office for Civil Rights (OCR). After considering a new round of public comments, HHS proposed organizational and substantive modifications to the Rule in March 2002. These editions principally sought to improve provisions that may have impeded patient access to delivery of quality health care. HHS adopted a final Privacy Rule in August 2002 with various modifications.

Though various federal bills to protect health information privacy continue to circulate on Capitol Hill, implementation of the new Privacy Rule will go forward. The Rule takes effect for most covered entities on April 14, 2003, and a year later for small health plans. Modifications to the Rule may occur in the next year as well.

Who is Covered?

HHS’ authority to issue health information privacy regulations was limited by Congress through HIPAA to a defined set of persons.\textsuperscript{13} The Rule thus applies to specific “covered entities” and their “business associates.” Covered entities include:

- **Health care providers** – a provider of medical or health services, and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. Health care providers (e.g., physicians, hospitals, clinics) are covered if they “transmit any health information in electronic form in connection with a transaction covered by [the Rule].”\textsuperscript{14} Electronic exchanges can include billing and fund transfers as well as communications containing health information.

- **Health plans** – an individual or group plan that provides, or pays the cost of, medical care which includes the diagnosis, cure, mitigation, treatment or prevention of disease. Health plans include private entities (e.g., health insurer, managed care organization) or government organizations (e.g., Medicaid, Medicare, the Veterans Administration);\textsuperscript{15} and

- **Health care clearinghouses** - a public or private entity, including a billing service, re-pricing company, community health information system, and “value-added” switches, that (1) process non-standard data into standard data elements or standard
transactions and/or (2) receive and process health information into non-standard format.\textsuperscript{16}

The Rule also applies to “business associates” (e.g., lawyers, accountants, billing companies, and other contractors) whose relationship with covered entities requires the sharing of PHI.\textsuperscript{17} Covered entities must assure that their business associates comply with privacy standards. Generally, a covered entity may, pursuant to a written agreement with its business associates, disclose PHI to these persons and allow them to use, create, or receive PHI on the entities’ behalf. The use or further disclosure of PHI by a business associate requires, among other things, the covered entity to obtain satisfactory assurances that the associate will appropriately safeguard the information. If a covered entity knows of a privacy violation by a business associate and fails to address it, the entity will be considered in violation of the Privacy Rule. Through these oversight functions, HHS can regulate some of the downstream users and processors of PHI.

**Who is Not Covered?**

Though comprehensive in its coverage, not all persons or entities that regularly use, disclose, or store identifiable health data are covered. The Rule, for example, does not cover employers, many insurers (including auto, life, and worker compensation insurers), or public agencies that deliver social security or welfare benefits even though these entities regularly use and disclose personal medical information. As discussed later, the Rule also does not directly apply to public health authorities or health researchers, though it impacts these health data users in external and internal ways.

**What Information is Protected?**

The Rule explicitly covers “protected health information” (PHI), which is largely defined as *individually identifiable health information*. Health information is data that are:

1. 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. related 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.\textsuperscript{18}

*Individually-identifiable health information* is any health information which “identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.”\textsuperscript{19} This definition is intentionally broad in scope. It includes any health data that contain uniquely identifiable characteristics (e.g., name, social security or drivers’ license number, address, fingerprint, or genetic link). Similar health information in education and certain other records subject to the Family Educational Rights and Privacy Act (FERPA) is not considered to be PHI under the Privacy Rule.

The text box below provides a listing of the 18 data elements defined as specific individual identifiers by the Rule.\textsuperscript{20} The inclusion of one or more of these identifiers within a
medical record meets the definition of PHI and requires the covered entity to comply with the provisions of the Rule.

<table>
<thead>
<tr>
<th>Comprehensive Set of Individual Identifiers Under the Privacy Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Names</td>
</tr>
<tr>
<td>2. All geographical subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes</td>
</tr>
<tr>
<td>3. All elements of dates directly related to an individual</td>
</tr>
<tr>
<td>4. Telephone numbers</td>
</tr>
<tr>
<td>5. Fax numbers</td>
</tr>
<tr>
<td>6. Electronic mail addresses</td>
</tr>
<tr>
<td>7. Social security numbers</td>
</tr>
<tr>
<td>8. Medical record numbers</td>
</tr>
<tr>
<td>9. Health plan beneficiary numbers</td>
</tr>
<tr>
<td>10. Account numbers</td>
</tr>
<tr>
<td>11. Certificate/license numbers</td>
</tr>
<tr>
<td>12. Vehicle identifiers and serial numbers including license plate numbers</td>
</tr>
<tr>
<td>13. device identifiers and serial numbers</td>
</tr>
<tr>
<td>14. Web Universal Resource Locaters (URLs)</td>
</tr>
<tr>
<td>15. Internet Protocol (IP) address numbers</td>
</tr>
<tr>
<td>16. Biometric identifiers including finger and voice prints</td>
</tr>
<tr>
<td>17. Full face photographic images and any comparable images, and</td>
</tr>
<tr>
<td>18. Any unique identifying number, characteristic, or code</td>
</tr>
</tbody>
</table>

PHI includes all mediums of health information, including electronic, oral, and paper communications. Protecting all the mediums of health information recognizes the impracticability of separating paper-based records from electronic or oral-based data. Incomplete coverage would leave a significant amount of health communications unregulated and complicate enforcement.

What Information is Not Protected?

De-identifiable data (e.g., aggregate statistical data, non-linked data, or data stripped of individual identifiers) require no individual privacy protections, and thus are not covered by the Privacy Rule. Covered entities may also use or disclose a “limited data set” for research, public health, or health care operations with few restrictions. Health information in a limited data set is not directly identifiable, but it may contain more identifiers than truly de-identified data sets.

Exceptions for the use and disclosure of de-identified data, and to a lesser degree, limited data sets, provide incentives for covered entities and others to de-identify health information to diminish the risk of unauthorized disclosures and uses. The Rule requires that a covered entity seeking to use or disclose de-identified PHI determine that the information is not individually identifiable, either through:

- “statistical de-identification” – an expert using accepted analytical techniques concludes that the risk is very small that the information could be used, alone or in combination with other reasonably available information, to identify the subject of the information; or the
• **“Safe harbor method”** -- a covered entity (or its business associate) removes a comprehensive set of identifiers (see text box above) such that the remaining information cannot alone or in combination with other data identify the subject.

Working with de-identified data, however, has limited value to public health practitioners and others who rely on identifiable health information to accurately report test results or conduct short-term or longitudinal surveillance and other activities. As a result, the use of de-identified health information in many cases may not be possible.

**What Does the Rule Require?**

For covered entities using or disclosing PHI, the Privacy Rule provides a range of health information privacy requirements and standards that attempt to balance individual privacy interests with communal uses of such data. Numerous existing print and online sources thoroughly review these requirements, which vary in complexity, scope, and duration (see CDC HIPAA Guidance). This document only briefly summarizes these requirements.

Among its many provisions, the Privacy Rule requires covered entities to:

- Notify individuals about their privacy rights and how their PHI is used or disclosed;
- Adopt and implement internal privacy procedures;
- Train employees to understand these privacy procedures;
- Designate persons who are responsible for implementing privacy procedures;
- Maintain the security of PHI so that it is not readily available;
- Vest health consumers with a series of rights based on fair information practices.

As to the latter requirement regarding fair information practices, this includes rights to:

- **Access Protected Health Information.** Individuals have many rights regarding their PHI. These include on-site inspections of records and the provision of copies upon request. In most instances, covered entities must accommodate a request for access, or provide a fair and informed process in case of denials subject to review.  

- **Amend Protected Health Information.** Individuals can request amendments to correct inaccuracies or supply missing information in their PHI. If the covered entity agrees to the amendment, it must (1) identify the records that are affected, (2) append or provide a link to the amendment, (3) inform the individual that the amendment has been made; and (4) work with other covered entities or business associates who possess or receive the data to make the amendments.

- **Notice.** Individuals have the right to adequate notice of the uses and disclosures of PHI made by the covered entity, and to know the covered entity’s privacy and security policies and fair information practices requirements. Notices must be in plain
language, and clearly posted. Covered entities must make a good faith effort to provide this notice to the patient before the delivery of services.  

- **Accounting for Disclosures.** Covered entities are required to maintain an accounting of disclosures of PHI (other than for disclosures related to treatment, payment and health care operations, and other exceptions). The accounting includes the name of the person or entity who received the information (and their address if known), the date of the disclosure, a brief description of the information disclosed, and a brief explanation of the reasons for disclosure if not authorized by the patient. Patients have a limited right to receive an accounting over a six-year period before the date of the request.

**What Are the Provisions Regarding Uses and Disclosures?**

The Privacy Rule restricts the use and disclosure of PHI in various contexts, and applies minimum disclosure principles for virtually all disclosures. Thus, when using or disclosing PHI, a covered entity must make reasonable efforts to limit the information to the minimum necessary to accomplish its purpose.

**Required Disclosures**

A covered entity is required to disclose PHI in only two instances: (1) when an individual requests his PHI; and (2) when HHS needs PHI to investigate compliance with the Rule. In every other circumstance, certain uses and disclosures of PHI are permitted, but not required, by the Rule.

**Disclosures for Treatment, Payment, and Health Care Operations**

Uses and disclosures of PHI for standard health care transactions (e.g., TPO – including treatment, payment or health care operations – see text box below) are permitted without individual written authorization. HHS suggests that patients know and expect that these uses and disclosures occur as a regular part of the delivery of health services. As a result, the Rule does not seek formal consent for these standard transactions.

**Standard Transactions under HIPAA**

Involves the transmission of PHI between two parties to carry out financial or administrative activities related to healthcare. It includes the following types of information transmissions:

1. Healthcare claims or equivalent encounter information
2. Healthcare payment and remittance advice
3. Coordination of benefits
4. Healthcare claim status
5. Enrollment and disenrollment in a health plan
6. Eligibility for a health plan
7. Health plan premium payments
8. Referral certification and authorization
9. First report of injury
10. Health claims attachments
11. Other transactions that the HHS Secretary may prescribe by regulation
**Authorized Disclosures**

Outside the TPO context, covered entities generally have to obtain individual authorization for uses or disclosures of PHI. Individual authorizations must:

- specifically identify the PHI to be used or disclosed;
- provide the names of the persons or organizations who will make and receive the use or disclosures;
- explain the purpose for each request;
- notify individuals of their right to refuse without negative consequences to treatment or health plan eligibility (except under specific circumstances);
- be written in plain language;
- include an expiration date; and
- allow the individual a right to revoke at any time in writing (except where the covered entity has already relied on the authorization).

Advance written authorization for uses or disclosures of PHI for non-health care purposes is seen as an important privacy safeguard. Unwarranted disclosures to existing or potential employers, insurers (e.g., health, life, disability), commercial marketers, family members, friends, neighbors, or others can negatively affect an individual’s job status or opportunities, insurability, social status, or cause other harms. Individuals should have some right to control disclosures that can result in discrimination, stigmatization, or embarrassment.

**Permissible Disclosures without Authorization**

Some uses and disclosures of PHI are consistent with achieving important communal or societal goals as part of the Rule’s attempt to balance individual and communal interests. In recognition of these communal and societal goals, the Privacy Rule recognizes a series of exceptions to the written authorization requirement for disclosures. These include disclosures related to:

- **Law enforcement.** Law enforcement officials may receive PHI from covered entities pursuant to a court order, subpoena, or other legal order;
- **Judicial and Administrative Proceedings.** A covered entity may disclose PHI in a judicial or administrative proceeding in response to an order of the court or administrative tribunal or, in certain circumstances, a subpoena or discovery request;
- **Commercial marketing.** Covered entities may use or disclose PHI for face-to-face commercial marketing to individuals or regarding products or services of nominal value;
- **Parents of unemancipated minors.** As personal representatives of unemancipated minors, parents are entitled to some disclosures of their minor’s PHI;
- **Family members, friends, and caretakers (“significant others”) of adults and emancipated minors.** Covered entities may disclose limited health information of an adult or emancipated minor to a relative, personal friend, or designated person in the case of an emergency or in the course of the significant other’s basic care-taking duties.
• **Public health.** PHI can be disclosed to public health authorities for public health purposes; and

• **Health research.** A covered entity can use or disclose PHI for research without consent if it obtains a waiver from an Institutional Review Board (IRB) or a privacy board according to a series of considerations.

**Does the Rule Preempt State or Local Laws?**

As a federal regulatory standard, the Privacy Rule provides a national floor of protections. As such, it preempts contrary state or local privacy laws. However, the Rule does not preempt state or local health information privacy laws that are more protective than the requirements or standards in the Privacy Rule. Thus, state or local privacy laws that provide greater protections of health information privacy than the Rule remain in effect. Laws that provide less protection do not.

The Privacy Rule specifically does not override state or local public health laws that provide for “the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.” Thus, state public health laws that require or authorize the disclosure of PHI for public health purposes or govern the privacy and confidentiality of public health information remain. As discussed later, this allows state and local public health authorities to continue to request and receive PHI from covered entities under the Privacy Rule.
IMPACT OF THE PRIVACY RULE ON PUBLIC HEALTH LABORATORIES

The Privacy Rule does not specifically define federal, tribal, state, or local public health authorities as “covered entities” that are principally subject to the Rule’s provisions. Further, HHS attempts to avoid interfering with public health activities that rely on PHI acquired, used, or disclosed by covered entities by, among other things, (1) permitting PHI disclosures for public health purposes to public health authorities without individual written authorization, and (2) leaving intact state and local public health laws requiring disclosures of PHI.

However, the Rule affects the traditional ways that PHI is used and exchanged among public health authorities. As covered entities prepare to comply with the Rule, some indications are that the Rule may impede the flow of PHI to public health authorities despite the Rules’ clarity on sharing this information. Covered entities are mistakenly starting to refuse to share PHI with public health authorities for public health purposes. These external barriers may limit public health’s access to and use of PHI. Some public health authorities may also perceive that the Rule affects how they utilize PHI once it has been received from covered entities. In addition, internal, operational barriers may result from the Rule since it may apply to specific functions of public health authorities. These external and internal impacts of the Rule on public health authorities are further discussed below.


One of the pervasive questions concerning the external impact of the Privacy Rule on public health practice is whether the Rule limits the disclosure of PHI by covered entities to public health authorities or their contractors/partners for public health purposes. The Rule specifically permits the disclosure of PHI to public health authorities for public health purposes without written authorization. Additional provisions for disclosures without authorizations for health research purposes may also apply.

What Is A Public Health Authority?

A public health authority is broadly defined as an “agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency . . . that is responsible for public health matters as part of its official mandate.” Public health authorities include federal public health agencies (e.g., CDC, NIH, FDA, OSHA); tribal health agencies; state public health agencies (e.g. public health departments or divisions, state cancer registries, vital statistics departments); local public health agencies; and anyone acting under authorization from or pursuant to a contract with a public health authority. State or local public health laboratories are likely also deemed “public health authorities” under this broad definition, even if they perform some “covered functions.” As discussed below, many public health laboratories may be considered “hybrid entities” because they have dual functions.

This definition recognizes that public health authorities often carry out their authorized activities with other partners using a variety of mechanisms such as contracts, grants, and
memoranda or letters of agreement. The Privacy Rule allows these partners to act as a public health authority for purposes of carrying out these functions. A covered entity may disclose PHI to these entities to the same extent it would be permissible to disclose PHI to a governmental public health authority. A covered entity may rely on documentation that the person or entity is acting as a public authority, such as a letter on the letterhead of the public health agency, or a copy of the contract or other agreement.

**Permitted Disclosures for Public Health**

The Rule allows disclosures of PHI to public health authorities when required by federal, tribal, state, or local laws (45 C.F.R. § 164.512(a)), or as permitted via common practice (45 C.F.R. § 164.512(b)). As HHS’ OCR clarifies in its interpretation of these corresponding sections of the Rule:

The . . . Rule permits covered entities to disclose the amount and type of [PHI] that [are] needed for public health purposes. In some cases, the disclosure will be required by other law, in which case, covered entities may make the required disclosure pursuant to 45 CFR 164.512(a) of the Rule. For disclosures that are not required by law, covered entities may disclose, without authorization, the information that is reasonably limited to that which is minimally necessary to accomplish the intended purpose of the disclosure.”

The Rule thus provides in Section 164.512(a) that disclosures of PHI may be made whenever they are required by law. This includes laws, like state public health reporting statutes, mandating disclosures of identifiable health data for public health purposes. This does not mean that a public health authority must have multiple disease- or condition-specific laws that authorize each collection of information. Many public health authorities operate under broad mandates to protect the health of the population; collection of health information is integral to this mandate. It is within the purview of the public health authority to determine the scope and effect of the laws within their jurisdiction.

**Other Permissible Disclosures without Authorization**

In other circumstances, Section 164.512 of the Rule permits covered entities to disclose PHI without individual authorization for specific public responsibilities that may have public health implications, including:

- emergency circumstances;
- identification of the body of a deceased individual, or the cause of death;
- oversight of the healthcare system;
- entities engaged in organ procurement, banking, or transplants; and
- activities related to national defense and security.

Once PHI is disclosed to a public health authority pursuant to these provisions, it is no longer covered by the Privacy Rule, and may be maintained, used, and disclosed consistent with the laws, regulations, and policies applicable to the public health authority. Thus, provided that
state law permits the sharing of such data by public health authorities across state boundaries, or among intrastate agencies, these disclosures may continue unabated by the Rule.

Other Requirements for Covered Entities

Though the Rule does not limit disclosures of PHI to public health authorities, it requires covered entities to log these and many other disclosures. \(^{38}\) This “accounting” requirement, in part, applies to uses and disclosures made to public officials and most disclosures mandated by law. It generally requires a covered entity to document disclosures over a six year period. An accounting is not required for disclosures made:

- for treatment, payment, and health care operations;
- in limited data sets via data use agreements;
- pursuant to individual written authorization;
- for standard health care transactions; or
- to the individual.

While accounting requirements apply to disclosures for public health purposes, the extent of the requirement varies. Concerning non-regular, specific, individual disclosures of PHI to public health authorities, a covered entity must generally document the date, recipient, address, and purpose or use. The vast amount of data exchanged between covered entities and public health authorities, however, is made through ongoing, regular reporting or inspection requirements. PHI may be disclosed to (or accessed by) public health authorities multiple times within a certain period of time. In these cases, a covered entity is not expected to log (or account) for each and every disclosure. Rather, it may simply provide requesting individuals with a general description of the first occurrence of public health disclosure and a statement as to the regular, ongoing sharing of PHI for public health purposes.

Under this modified accounting requirement for multiple disclosures of PHI to the same public health agency for the same purpose, covered entities can utilize an abbreviated accounting procedure. In some cases, public health authorities can assist covered entities in meeting this accounting requirement by providing summary information.

In addition, for disclosures of PHI for research purposes without individual authorization involving at least 50 records, the Rule allows for a simplified accounting by covered entities. Covered entities may provide individuals with a list of all protocols for which the patient’s PHI may have been disclosed, as well as the researcher’s name and contact information. Of course, if the disclosure is made as a limited data set, an accounting is not required.

The “Minimum Necessary” Standard

The Rule requires covered entities to limit the amount of data disclosed to the minimum necessary to achieve the specified goal. \(^{42}\) Covered entities can establish a minimum necessary policy that governs how PHI will be released by the covered entity. Alternatively, the Rule permits covered entities to reasonably rely on a requested disclosure as the minimum necessary for the stated purpose(s) based on the discretion of other covered entities or their business
associates, health researchers, and public health authorities. This allows covered entities to rely on public health officials to define what is minimally necessary for the stated purpose of the disclosure.44

**Internal Impact – Public Health Laboratories Authorities Performing Covered Functions**

Public health authorities or their contractors/partners at the federal, tribal, state, or local levels that perform public health functions are not subject to the Rule’s provisions. Thus, a state public health department that uses PHI to conduct public health surveillance does not have to adjust its practices to adhere to the Rule. These authorities are simply not covered by the Rule.

What if the public health authority, however, acts like a covered entity, or otherwise meets the definition of a covered entity as a health plan, health care provider, or health care clearinghouse? Public health authorities or their contractors/partners that perform “covered functions” (like the provision of health care or services, or insuring persons for health care costs) are subject to the Rule’s provisions.

**Do Public Health Laboratories Perform Covered Functions?**

Whether state or local public health laboratories perform “covered functions,” and thus must adhere to the Rule’s requirements, is a key issue. For the purpose of this analysis, the definition of “public health laboratory” includes those facilities operating as part of a state or local public health system either as a component of a larger governmental public health agency, or as a private sector entity that directly contracts with (or receives grant funds from) such an agency, which performs laboratory testing on human specimens to provide information for the diagnosis, prevention, treatment of disease or impairment, or assessment of health.

Many state and local public health laboratories have considered whether they perform covered functions, often in conjunction with their larger public health agencies. Decisions as to whether state and local public health labs perform “covered functions” vary. Some see themselves (or have been advised by state counsel) as exempt from the Privacy Rule because they:

- do not meet the definition of “health care provider” or “health plan;”
- do not submit electronic claims for payment; and/or
- do not provide services directly to the patient.

In other states, public health labs are deemed “covered” either because they do some things other labs do not (e.g., provide lab results directly to patients and/or bill electronically), or their larger public health agency has declared itself as “covered.”

The incentive to label public health lab services as non-covered functions under the Privacy Rule is clear: public health labs may not want to have to adhere to the additional requirements of the Rule, even if these requirements largely comport with their existing privacy practices.
If public health laboratories may be seen as performing “covered functions,” it is unlikely that the functions they perform are like those of a “healthcare clearinghouse.” Public health labs do not gather PHI for the purpose of filtering, processing, or reconstituting the data. It is also unlikely that a public health lab would be seen as a “health plan.” Labs do not insure persons against their potential health risks, nor reimburse health providers or otherwise fund them to perform direct health care services.

**Public Health Laboratories as Health Care Providers**

Are the functions of public health laboratories “covered” under the “health care provider” prong of the definition of covered entity? A public health laboratory that provides medical or health care services as part of its activities may be considered a covered entity if it also performs standard transactions electronically (with PHI) as part of these activities.

“Health care” is very broadly defined in the Rule as “care, services, or supplies related to the health of an individual,” including preventive, diagnostic, rehabilitative, or maintenance care, and services, assessments, or procedures concerning the person’s physical or mental condition or status. This includes the performance of lab services on tissue or biologic samples to determine an individual patient’s diagnostic status or potential exposure to a disease or condition.

Yet, it may be important to examine the sorts of requests for laboratory services that a public health lab receives. Public health lab service requests may come directly from a covered entity, typically a physician or other health care worker (HCW). The lab provides its service and reports results directly to the requesting HCW (and sometimes the patient). In such cases, these services are part of the delivery of health services. If any of these transactions are conducted electronically (see text below), the lab is performing “covered functions.”

In contrast, a request for lab services may derive from another part of the public health agency. For example, in the process of investigating an infectious disease outbreak, the state public health agency may request the state public health lab to test a series of patient samples for a specific infectious agent. The test results may be relayed directly to the state public health agency as part of the agency’s epidemiological investigation. These lab activities may be conducted in pursuit of a public health goal (e.g., assisting in an epidemiological investigation). Under these instances, the public health lab services may arguably be seen as “public health activities.”

Despite distinctions between the sources of lab requests, the focus of the Rule’s coverage is on the provision of health services to the individual. Anyone who performs these services, for largely public health purposes or otherwise, may be considered as performing “covered functions.” Underlying each of these examples is the delivery of some level of health services to individual patients who may have been exposed to the disease. In the first example, the covered entity and the lab provide health services to an individual. In the second example, the state public health agency and its lab provide individual health services. In both cases, individual privacy rights under the Rule may thus apply. The application of these rights, however, would not prevent the lab from directly reporting the test results to the state public health agency because of the public health provisions allowing disclosures without written authorization.
Public Health Laboratories and Electronic Transmissions

The Rule applies to anyone who furnishes, bills, or is paid for covered, healthcare functions provided they “transmit any health information in electronic form in connection with a transaction covered by [the Rule].” Like the provision of health services, a covered “transaction” under the Rule is broadly defined (see text box above). Electronic exchanges can include billing and fund transfers in addition to communications containing health information.

A transaction is specifically defined as the transmission of information between two persons to carry out financial or administrative activities related to health care. This includes transmissions regarding health care claims or encounter information; health care payment and remittance advice; coordination of benefits; health care claim status; first report of injury; health claims attachments; and other transactions that HHS may decide.

Through broad definitions and corresponding interpretations of the Rule, HHS attempts to apply the Rule to as many health providers as possible. Essentially, any health provider who conducts electronic transactions as part of the delivery of its health services is covered by the Rule. Once the determination of coverage is made, the Rule applies to all mediums of PHI acquired, used, or disclosed.

Public Health Laboratories as Hybrid Entities

1. What if one part or division of a public health authority is subject to the Rule because it performs covered functions – is the entire authority required to adhere to all of the provisions of the Rule? Yes, unless the public health authority adopts a “hybrid entity” status.

If an organization determines that it has programmatic functions that fall within the Privacy Rule’s framework, it must designate itself a covered entity under the Privacy Rule. If the organization also determines that it performs programmatic functions not covered by the Privacy Rule (e.g., public health surveillance, interventions, and/or investigations), the organization may designate itself a hybrid entity.

Once an organization designates itself a hybrid entity, the Privacy Rule provisions apply only to the covered functions of the authority. This designation permits organizations to erect an administrative firewall between covered and non-covered functions. By doing so, they can avoid the application of Privacy Rule requirements on all facets of their activities and limit additional administrative burdens to covered functions.

A public health authority that elects to designate itself a covered entity (but not a hybrid entity) will be required to fully comply with all of the Privacy Rule requirements. Although this would not preclude a public health authority from continuing to conduct authorized public health functions, it may seriously complicate data handling and impede the flow of PHI.
Additional Roles for Public Health Laboratories

In addition to providing test results for individual patients, state and local public health laboratories in many jurisdictions have other functions. They may provide lab services for the state or local government’s food, drinking water, air, wastewater, and hazardous waste programs. In each of these capacities, the lab is not performing covered functions provided that it is not engaged in providing health services to individuals.

What about state public health labs that also operate the state forensics labs? These labs are regularly asked to interface with law enforcement authorities to provide forensic data that may help identify persons or victims of a crime. They may also perform autopsies to determine causes of death pursuant to a specific law enforcement request. Is information related to an autopsy performed by a state public health lab covered by the Privacy Rule? Yes. The Rule specifically applies to the PHI of deceased individuals.\(^{51}\) There are, however, multiple exceptions concerning uses and disclosures of PHI regarding autopsy information including:

♦ The disclosure of autopsy data to law enforcement authorities for the purpose of identifying victims of a crime;\(^ {52}\)

♦ The disclosure of such data to law enforcement authorities for the purpose of alerting law enforcement of the suspicion of a crime;\(^ {53}\) or

♦ The sharing of PHI between other covered entities and the coroner or medical examiner for the purpose of identifying the deceased, determining a cause of death, or other legally-authorized duties.\(^ {54}\)

Individual Access Rights Regarding PHI Held by Public Health Laboratories

As stated above, when public health laboratories provide clinical lab services for the benefit of individual patients, they are covered under the Rule just like other covered entities. In some cases, however, the Rule excludes select persons providing covered functions from all or part of the Rule’s requirements. One example are the Privacy Rule’s requirements regarding patient access and the Clinical Laboratory Improvements Amendments of 1988 (CLIA).

The Rule states that an individual has a right of access to inspect and obtain copies of their PHI, except for PHI held by a covered entity that is (1) subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA) to the extent that individual access would be prohibited by law; or (2) a research laboratory that tests human specimens but does not report patient-specific results under CLIA (42 CFR 493.3(a)(2)).\(^ {55}\)

The Privacy Rule, thus, does not require public health laboratories performing covered functions to provide an individual access to information if CLIA or authorized state laws prohibit them from doing so. CLIA permits clinical laboratories to provide lab test records and reports only to “authorized persons,” as defined by state law. In some states, “authorized persons” include the individual who is the subject of the PHI; in other states, they do not. If state law does
not define who is an “authorized person,” CLIA defines it as the person who orders the test (in general, a health care provider).

In addition, for certain research laboratories that are exempt from CLIA, the Rule does not require them to provide individuals with access to PHI where doing so may result in the lab losing its CLIA exemption.\textsuperscript{56}

In short, if state or federal law allows individual access to PHI held by the labs under CLIA, the Rule’s access provisions apply. If state or federal law does not allow individual access through the lab under CLIA, the Rule does not either. This does not mean an individual lacks any access to the lab results. As HHS acknowledges, “. . . in most cases, individuals . . . will be able to receive their test results or reports through the health care provider who ordered the test . . . [a]ssuming that the provider is a covered entity.”\textsuperscript{57}

\textbf{Conclusion}

The Privacy Rule introduces new standards for protecting the privacy of individually-identifiable health information. For covered entities and those providing “covered functions,” the Privacy Rule sets national minimum standards for how PHI is used and disclosed and provides individuals some level of control and knowledge over their health information.

Although public health laboratory practices are not the target of the Rule, it affects these practices in external and internal ways. The ability of a public health laboratory to access PHI after April 14, 2003 may be hindered by covered entities that rely on misinterpretations of conservative interpretations of what is permissible under the Privacy Rule. State and local public health laboratories that provide covered functions may have to adhere to many of the Rule’s requirements if they also conduct transactions electronically. Many labs and their larger health agencies may seek to establish themselves as hybrid entities to minimize the impact of the Rule.

The guidance in this document is designed to assist public health laboratory practitioners to comply with the Privacy Rule. Please note that this document cannot replace the interpretations and decisions of state or local government counsel or others empowered with the duty to enforce the Rule. As well, as with any new set of federal regulations, interpretations may vary and change based on administrative needs and decisions, legislative actions, and judicial decisions.
Appendix A – Glossary of Terms

**Accounting** – An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures (a) to carry out treatment, payment and health care operations, (b) to individuals of protected health information about them, (c) for the facility’s directory or to persons involved in the individual’s care or other notification purposes, (d) for national security or intelligence purposes as provided in §264.512(k), or (e) that occurred prior to the compliance date for the covered entity. Such an accounting must meet the following requirements: (1) the accounting must include disclosures of protected health information that occurred during the six years prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity; (2) the accounting must include for each disclosure: the date of the disclosure, the name of the entity or person who received the protected health information, and if known, the address of such entity or person; a brief description of the protected health information disclosed; and, 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 a statement, a copy of the individual’s written authorization pursuant to §164.508, or a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §164.502(a)(2)(ii) or §164.512, or pursuant to a single authorization under §164.508, the accounting may, with respect to such multiple disclosures provide the information required by paragraph (b)(2) of §164.528 for the first disclosure during the accounting period, the frequency, periodicity, or number of the disclosures made during the accounting period, and the date of the last such disclosure during the accounting period. §164.528.

Modified accounting procedures are also provided for covered entities making research disclosures involving more than 50 persons.

**Business associate** – a person who . . . assists in the performance of . . . a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or . . . provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. §160.103.

**Covered entity** – means (1) a health plan; (2) a health care clearinghouse; (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Rule. §160.103.

**Covered functions** – those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse. §164.501.

**Disclosure** – the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. §164.501.
Electronic Form – using electronic media, as that term is defined at §162.103. It includes transmissions over the internet, extranet, leased lines, dial-up lines, and private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disc, or CD media. §162.103.

Health Care – care, services, or supplies related to the health of an individual. It includes but is not limited to: (1) preventive, diagnostic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and, (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. §160.103.

Health care clearinghouses -- a public or private entity, including a billing service, re-pricing company, community health information system, and “value-added” switches, that (1) process non-standard data into standard data elements or standard transactions and/or (2) receive and process health information into non-standard format. §160.103.

Health care Provider -- a provider of services, a provider of healthcare services, and any other person or organization that furnishes, bills, or is paid for healthcare in the normal course of business. §160.103.

Health information -- any 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 condition of an individual, or the past, present, or future payment for the provision of health care to an individual. §160.103.

Health plan -- means an individual or group plan that provides, or pays the cost of, medical care, which includes the diagnosis, cure, mitigation, treatment or prevention of disease. Health plan includes the following, singly or in combination: (i) a group health plan; (ii) a health insurance issuer; (iii) an HMO; (iv) Part A or B of the Medicare program under title XVIII of the Act; (v) the Medicaid program under title XIX of the Act; (vi) an issuer of Medicare supplemental policy; (vii) an issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy; (viii) an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers; (ix) the health care program for active military personnel under title 10, U.S.C.; (x) the veterans health care program under 38 U.S.C. Ch. 17; (xi) the Civilian Health and Medical Program of the Uniformed Services; (xii) The Indian Health Service program under the Indian Health Care Improvement Act; (xiii) The Federal Employees Health Benefits Program; (xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act; (xv) the Medicare+ Choice program under Part C of title XVIII of the Act; (xvi) a high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals; (xvii) any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care. §160.103.

The term health plan does not include: (i) any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in §2791(c)(1) of the PHS Act; and, (ii) a government-funded program whose principal purpose is other than providing, or paying the cost of, health care, or whose principal activity is (1) the direct provision of health care to persons; or (2) the making of grants to fund the direct provision of health care to persons. §160.103.

Hybrid entity – a single legal entity that (1) is a covered entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates health care components in accordance with paragraph (c)(3)(iii) of this section. §164.504.
Individually identifiable health information (IIHI) -- 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, or the past, present, or future payment for the provision of health care to an individual; and, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual. §164.501.

Limited data set – protected health information that excludes certain direct identifiers of the individual or of relatives, employers, or household members of the individual. (Direct identifiers to be excluded can be found in §164.514(e)(2)). §164.514.

Minimum Necessary – means that for any type of disclosure that a covered entity makes on a routine and recurring basis, that the covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, covered entities must develop and implement criteria designed to limit the protected health information 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. A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when (a) making disclosures to public officials that are permitted under §164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose, (b) if the information is requested by another covered entity (c) their business associates or (d) documentation or representations that comply with the applicable requirements of §164.512(i) have been provided by a person requesting the information for research purposes. §164.514(d)(3).

Non-Identifiable data – health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. §164.514(a).

Payment – (1) The activities undertaken by: (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) relate to the individual to whom health care is provided and include, but are not limited to: (i) determinations of eligibility or coverage...and adjudication or subrogation of health benefit claims ; (ii) risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance), and related health care data processing; (iv) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (a) name and address; (b) date of birth; (c) social security number; (d) payment history; (e) account number; and (f) name and address of the health care provider and/or health plan. §164.501.

Protected Health Information (PHI)-- individually identifiable information about the past, present, or future physical or mental health of an individual that is transmitted by electronic media, maintained in any medium described in the definition of electronic media, or transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in (“health plans” means an individual or group plan that provides, or pays the cost of, medical care which includes the diagnosis, cure, mitigation, treatment or prevention of disease (i) education records covered by the Family Education

**Public health authority** -- an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention (CDC), and the Occupational Safety and Health Administration (OSHA). §164.501.

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

**Statistical de-identification** -- an expert using accepted analytical techniques can conclude that the risk is very small that the information could be used, alone or in combination with other reasonably available information to identify the subject of the information. §164.514(b).

**Safe harbor method** -- a covered entity or its agent removes a comprehensive set of identifiers enumerated in the Privacy Rule, which includes but is not limited to, names, geographic subdivisions smaller than states, dates more specific than years, contact information, identification numbers and photographic images, and has no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is a subject of the information, or the individual’s relatives, employers, or household members. Eighteen specific identifiers will need to be removed to achieve de-identification. §164.514(b).

**Transaction** – the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: health care claims or equivalent encounter information; health care payment and remittance advice; coordination of benefits; health care claim status; enrollment and disenrollment in a health plan; eligibility for a health plan; health plan premium payments; referral certification and authorization; first report of injury; health claims attachments; other transactions that the secretary may prescribe by regulation. §164.103.

**Treatment** – the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. §164.501.

**Use** -- with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. §164.501.
References

10. 45 C.F.R. § 164.512(b)
13. 45 C.F.R. § 160.102.
15. 45 C.F.R. § 160.103
16. Ibid.
17. Ibid.
18. Ibid.
19. 45 C.F.R. § 164.501
20. 45 C.F.R. § 164.514(b)(2)(i)
21. 45 C.F.R. § 164.514(a)
22. 45 C.F.R. § 164.514
23. 45 C.F.R. § 164.514(b)
24. 45 C.F.R. § 164.504
25. 45 C.F.R. § 164.524
26. 45 C.F.R. § 164.526
27. 45 C.F.R. § 164.520
28. 45 C.F.R. § 164.528
29. 45 C.F.R. § 164.502(a)
30. 45 C.F.R. § 164.502(a)(2)
31. 45 C.F.R. § 164.506
32. 45 C.F.R. § 164.512
33. 45 C.F.R. § 160.202
34. 45 C.F.R. § 164.501
35. 45 CFR 164.512 (a)
36. 45 C.F.R. § 164.528
37. 45 C.F.R. Section 164.514(d)(1)
38. 45 C.F.R. Section 164.514(d)(3)(iii)
39. 45 C.F.R. § 160.102(a)(3).
40. 45 C.F.R. § 164.504
51. 45 C.F.R. § 164.502[f]
For more information, see HHS HIPAA Questions and Answers, available at http://answers.hhs.gov/.