Individual's Right Under HIPAA to Access their Health Information (HHS Guidance)

Provides individuals with a legal, enforceable right to see and receive copies, upon request, of the information in their medical and other health records maintained by their health care providers and health plans.

Updated last **July 12, 2017**
for the 01/07/2016 guidance.

WHAT IT DOES

"Individual's Right Under HIPAA to Access their Health Information" is a guidance issued by the Department of Health and Human Services Office of Civil Rights (OCR) to clarify section 164.524 of the HIPAA Privacy Rule (45 CFR 160 and Subparts A and E of 45 CFR 164). This guidance outlines the right of patients to request their Protected Health Information (PHI) from a HIPAA covered entity (e.g., health plan or care provider) and receive it in a timely manner. The OCR indicated that the guidance was released in response to "obstacles" faced by patients, and called it "an important step toward ensuring that individuals can take advantage of their HIPAA right of access."

The guidance consists of a fact sheet for the regulations found in 45 CFR 164.524 as well as a number of frequently asked questions (also found here), which consider how the regulations would apply in various scenarios. The right to access covers both the right of an individual (or their personal representative) to inspect and obtain a copy of their PHI, as well as the right to have their PHI directly transmitted to a third party of their choice. It also places emphasis on the obligations of the covered entity to meet the specifics of the individual's request for access, within reason. Of special note to clinical researchers, the right to access sometimes applies to research records or results.

A detailed outline of the guidance is given below.

Information subject to the right of access:

- An individual's PHI contained within a "designated record set", (defined in 45 CFR 164.501), which in general is "a group of records maintained by or for a covered entity" and "used in whole or in part to make decisions about the individual."
  - Includes medical records, billing and payment records, clinical lab test results (like genetic tests), medical images like x-rays, clinical case notes, etc.
- When access is requested, the covered entity is not required to create new information, explanations, or analyses that are not already in the designated record set.

As HHS explicitly states, in order for genetic information (e.g. genetic test results or medical history) to be covered under HIPAA, "it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse." For example, an individual might request access to their genetic data that is maintained by a clinical laboratory. As the guidance states, "a clinical laboratory that is a HIPAA covered entity and that conducts next generation sequencing (NGS) of DNA on an individual must provide the individual, upon the individual's request for PHI concerning the NGS, with a copy of the completed test report, the full gene variant information generated by the test, as well as any other information in the designated record set concerning the test."

Information excluded from the right of access:

- PHI that is not used to make decisions about the individual (and thus not part of a designated record set), such as quality assessment, management records used for business decisions (like performance evaluations), business planning, etc.
- Psychotherapy notes, which are personal notes from a mental health professional maintained separately from the patient's

medical record
- Information compiled in anticipation of, or for use in, a civil, criminal, or administrative action or proceeding

The covered entity is allowed to require a written request, electronic request, or request via a form specific to the entity, as long as it does not create a barrier to access or unreasonably delay access. Furthermore, the covered entity must take "reasonable steps" to verify the identity of the individual requesting access. The methods of verification are discretionary, but must comply with 45 CFR 164.312 (d) of the HIPAA Security Rule and cannot bar or unreasonably delay the individual's access to their PHI.

In regards to providing access, the covered entity:

- Must supply the PHI to the individual in the form and format requested (e.g., on paper or electronically, file types, etc.), or if not, in a readable hard copy form. The covered entity must also arrange a convenient meeting, or transfer via mail, electronically, or other agreed upon method to facilitate access (all covered entities are expected to be capable of mail or e-mail transfer).
  - Example: If the individual requests the PHI in a paper format and the PHI is maintained electronically, the covered entity must provide the PHI in a paper format unless it is not readily producible in that format
- Is not expected to tolerate unacceptable levels of risk to the security of its systems when it is facilitating access.
- Must provide access no later than 30 calendar days after receiving the request. If necessary, covered entities can extend the period by an additional 30 days if the individual is notified with written explanation of the delay and the date by which access will be provided.
- Is allowed to provide a summary in lieu of access, or an explanation in addition to access, if that has been agreed to by the individual.
- May charge a fee covering the following:
  - Labor for copying the PHI, regardless of form;
  - Supplies for creating the copy;
  - Postage; and
  - Preparation of an explanation or summary, if agreed upon.

A covered entity may deny access to all or a portion of a request under certain circumstances. Such denials are optional (not mandatory).

- Unreviewable grounds for denial (45 CFR 164.524(a)(2)):
  - Request for psychotherapy notes or information compiled for legal proceedings
  - Requested PHI is part of an ongoing research study that includes treatment. This is only valid if the patient agreed to suspension of access when consenting to participate in the research. The right to access must be reinstated after the research is completed.
  - Inmate's request of information that would jeopardize the health, safety, security, custody or rehabilitation of the inmate, other inmates or staff (the inmate can still inspect their PHI).
  - Requested PHI is in Privacy Act (5 U.S.C. 552a) protected records, maintained by a federal agency or a contractor to a federal agency
  - Requested PHI was obtained from someone other than a healthcare provider (like a family member) under the promise of confidentiality and providing access to the information would be reasonably likely to reveal the source of the information
- Reviewable grounds for denial (45 CFR 164.524(a)(3))
  - Requested PHI is reasonably likely to endanger the life or physical safety of the individual or another person.
  - Requested PHI is reasonably likely to cause substantial harm (defined in 65 Federal Register 82556 as physical, emotional, or psychological harm) to another person mentioned in the PHI (other than a health care provider).
  - Granting access to an individual's personal representative is reasonably likely to cause substantial harm to the individual or another person
- The covered entity may not require the individual to provide a reason for requesting access, or refuse on the grounds of that reason if offered.

The covered entity has certain obligations when carrying out a denial of access.

- The covered entity must provide a written denial no later than 30 days after the request, which in plain language describes the entity's reasoning and includes a protocol for filing a complaint or an appeal.
- After excluding the denied information, the covered entity must provide the individual with any other requested PHI it has, regardless of whether it is the complete requested set of information
- If the covered entity does not maintain the requested PHI, it must refer the individual to the entity that does

If a review of the denial is requested, the covered entity must promptly refer the request to a designated reviewing official and provide written notice to the individual of the determination of the reviewing official, as well as take other action as necessary.

All state laws that provide greater rights of access to PHI than the Privacy Rule, or that are not contrary to the Privacy Rule, are not preempted. However, those state laws that are contrary to the Privacy Rule are preempted.

RELEVANT SCIENCE

Genetic tests are lab tests used to detect an individual's genetic variants. Genetic variations contribute to the diversity of human appearance (eye color, height, etc.), but they also determine a person's susceptibility to a number of disorders. Some disorders can be caused by a single mutation, while other disorders might have more complex and multivariate genetic factors. Scientists have developed a number of genetic tests to detect known disease-causing or -associated genetic variations – these typically only examine one or a few of the more than 20,000 genes found in the human genome (the total DNA found in a human cell) at a time. However, technological advancements like next generation sequencing have opened the door for large-scale genetic tests that examine large portions or even the entirety of a patient's genome for genetic variation.

RELEVANT EXPERTS

Dr. Lawrence Muhlbaier, Office of Audit, Risk and Compliance, Associate Professor of Biostatistics and Bioinformatics, Duke University

"I have been working with the privacy aspects of HIPAA since 2000, when the privacy regulation was still in the proposal stage. Though my primary area is in enabling research in the context of the HIPAA Privacy Rule and the Common Rule, the interrelationship of all aspects of the Privacy Rule require a comprehensive view. The right of access is an important individual right that did not exist pre-HIPAA."

ENDORSEMENTS & OPPOSITION

Endorsements:

- The GetMyHealthData campaign issued a statement in general support of the guidance. Campaign coordinator Christine Bechtel said that the guidance is "an important step forward in helping patients exercise their right to access their health information under HIPAA, including electronically. Our cadre of volunteer 'Tracer' patients has found that, unfortunately, confusion surrounding HIPAA persists and often means that patients don't get the kind of access to their health care information they need. We are hopeful that the clarifications HHS issued yesterday will help both providers and patients better understand the law and the opportunities it presents. When all patients can get and use their health data electronically, they will be able to more fully engage in their health and care."

Opposition:

At present, there has not been any publicly reported opposition to this guidance.

STATUS

This guidance was published by the OCR on January 7, 2016 in conjunction with a statement from the OCR Director Jocelyn Samuels (archived here).

RELATED POLICIES

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted under Title XIII of the American Recovery and Investment Act of 2009. This act expanded the access to require electronic distribution of the requested records, and adopted a broader definition of Health Information Technology, outlined by HHS here.

POLICY HISTORY

This guidance was issued in connection to the Health Insurance Portability and Accountability Act (HIPAA). HIPAA became law in 1996 to enhance the portability and continuity of health insurance coverage, as well as to combat waste, fraud and abuse in health insurance and healthcare delivery.

In 2003, the HIPAA Privacy Rule (codified in 45 CFR 160 and Subparts A and E of 45 CFR 164) became effective, defining PHI and how it should be issued, maintained, and disclosed.

In 2005, the HIPAA Security Rule became effective, protecting electronically stored PHI (ePHI) and creating security protections for the data on an administrative, physical and technical level.

In 2006, the Enforcement Rule was implemented, giving HHS the power to combat breaches in compliance.

In accordance with 45 CFR 164.520, the covered entity must also communicate how they may use the patient's information and the patient's access rights in a Notice of Privacy Practices. (Example from Duke Health).

PRIMARY AUTHOR

Nicole Angelica, MA Candidate in Bioethics and Science Policy

EDITOR(S)

Hira Ahmed, MA Candidate in Bioethics and Science Policy, Alex Robeson, Ph.D.

RECOMMENDED CITATION

Duke SciPol, "Individual's Right Under HIPAA to Access their Health Information (HHS Guidance)" available at http://scipol.duke.edu/content/individuals-right-under-hipaa-access-their-health-information-hhs-guidance (07/13/2017).

LICENSE

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. Please distribute widely but give credit to Duke SciPol and the primary author(s) listed above, linking back to this page if possible.