Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524

Introduction

Providing individuals with easy access to their health information empowers them to be more in control of decisions regarding their health and well-being. For example, individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research. With the increasing use of and continued advances in health information technology, individuals have ever expanding and innovative opportunities to access their health information electronically, more quickly and easily, in real time and on demand. Putting individuals "in the driver's seat" with respect to their health also is a key component of health reform and the movement to a more patient-centered health care system.

The regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protect the privacy and security of individuals' identifiable health information and establish an array of individual rights with respect to health information, have always recognized the importance of providing individuals with the ability to access and obtain a copy of their health information. With limited exceptions, the HIPAA Privacy Rule (the Privacy Rule) 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.

General Right

The Privacy Rule generally requires HIPAA covered entities (health plans and most health care providers) to provide individuals, upon request, with access to the protected health information (PHI) about them in one or more "designated record sets" maintained by or for the covered entity. This includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. Individuals have a right to access this PHI for as long as the information is maintained by a covered entity, or by a business associate on behalf of a

covered entity, regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated (e.g., whether the covered entity, another provider, the patient, etc.).

Information Included in the Right of Access: The "Designated Record Set"

Individuals have a right to access PHI in a "designated record set." A "designated record set" is defined at 45 CFR 164.501 as a group of records maintained by or for a covered entity that comprises the:

- Medical records and billing records about individuals maintained by or for a covered health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals. This last category includes records that are used to make decisions about any individuals, whether or not the records have been used to make a decision about the particular individual requesting access.

The term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

Thus, individuals have a right to a broad array of health information about themselves maintained by or for covered entities, including: medical records; billing and payment records; insurance information; clinical laboratory test results; medical images, such as X-rays; wellness and disease management program files; and clinical case notes; among other information used to make decisions about individuals. In responding to a request for access, a covered entity is not, however, required to create new information, such as explanatory materials or analyses, that does not already exist in the designated record set.

Information Excluded from the Right of Access

An individual does not have a right to access PHI that is not part of a designated record set because the information is not used to make decisions about individuals. This may include certain quality assessment or improvement records, patient safety activity records, or business planning, development, and management records that are used for business decisions more generally rather than to make decisions about individuals. For example, a hospital's peer review files or practitioner or provider performance

evaluations, or a health plan's quality control records that are used to improve customer service or formulary development records, may be generated from and include an individual's PHI but might not be in the covered entity's designated record set and subject to access by the individual.

In addition, two categories of information are expressly excluded from the right of access:

- Psychotherapy notes, which are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session, that are maintained separate from the rest of the patient's medical record. See 45 CFR 164.524(a)(1)(i) and 164.501.
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. See 45 CFR 164.524(a)(1)(ii).

However, the underlying PHI from the individual's medical or payment records or other records used to generate the above types of excluded records or information remains part of the designated record set and subject to access by the individual.

Personal Representatives

An individual's personal representative (generally, a person with authority under State law to make health care decisions for the individual) also has the right to access PHI about the individual in a designated record set (as well as to direct the covered entity to transmit a copy of the PHI to a designated person or entity of the individual's choice), upon request, consistent with the scope of such representation and the requirements discussed below. See 45 CFR 164.502(g) and http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalreps.html for more information about the rights that can be exercised by personal representatives.

Requests for Access

Requiring a Written Request

A covered entity may require individuals to request access in writing, provided the covered entity informs individuals of this requirement. See 45 CFR 164.524(b)(1). Covered entities also may offer individuals the option of using electronic means (e.g., e-mail, secure web portal) to make requests for access. In addition, a covered entity may require individuals to use the entity's own supplied form, provided use of the form does not create a barrier to or unreasonably delay the individual from obtaining access to his PHI, as described below.

Verification

The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. See 45 CFR 164.514(h). The Rule does not mandate any particular form of verification (such as obtaining a copy of a driver's license), but rather generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity, provided the verification processes and measures do not create barriers to or unreasonably delay the individual from obtaining access to her PHI, as described below. Verification may be done orally or in writing and, in many cases, the type of verification may depend on how the individual is requesting and/or receiving access – whether in person, by phone (if permitted by the covered entity), by faxing or e-mailing the request on the covered entity's supplied form, by secure web portal, or by other means. For example, if the covered entity requires that access requests be made on its own supplied form, the form could ask for basic information about the individual that would enable the covered entity to verify that the person requesting access is the subject of the information requested or is the individual's personal representative. For those covered entities providing individuals with access to their PHI through web portals, those portals should already be set up with appropriate authentication controls, as required by 45 CFR 164.312(d) of the HIPAA Security Rule, to ensure that the person seeking access is the individual or the individual's personal representative.

Unreasonable Measures

While the Privacy Rule allows covered entities to require that individuals request access in writing and requires verification of the identity of the person requesting access, a covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonably delay the individual from obtaining access. For example, a doctor may not require an individual:

- Who wants a copy of her medical record mailed to her home address to physically come to the doctor's office to request access and provide proof of identity in person.
- To use a web portal for requesting access, as not all individuals will have ready access to the portal.
- To mail an access request, as this would unreasonably delay the covered entity's receipt of the request and thus, the individual's access.

While a covered entity may not require individuals to request access in these manners, a covered entity may permit an individual to do so, and covered entities are encouraged to offer individuals multiple options for requesting access.

Providing Access

Form and Format and Manner of Access

The Privacy Rule requires a covered entity to provide the individual with access to the PHI in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form or other form and format as agreed to by the covered entity and individual. See 45 CFR 164.524(c)(2)(i). If the individual requests electronic access to PHI that the covered entity maintains electronically, the covered entity must provide the individual with access to the information in the requested electronic form and format, if it is readily producible in that form and format, or if not, in an agreed upon alternative, readable electronic format. See 45 CFR 164.524(c)(2)(ii). The terms "form and format" refer to how the PHI is conveyed to the individual (e.g., on paper or electronically, type of file, etc.) Thus:

- Requests for Paper Copies – Where an individual requests a paper copy of PHI maintained by the covered entity either electronically or on paper, it is expected that the covered entity will be able to provide the individual with the paper copy requested.
- Requests for Electronic Copies –
- Where an individual requests an electronic copy of PHI that a covered entity maintains only on paper, the covered entity is required to provide the individual with an electronic copy if it is readily producible electronically (e.g., the covered entity can readily scan the paper record into an electronic format) and in the electronic format requested if readily producible in that format, or if not, in a readable alternative electronic format or hard copy format as agreed to by the covered entity and the individual.
- Where an individual requests an electronic copy of PHI that a covered entity maintains electronically, the covered entity must provide the individual with access to the information in the requested electronic form and format, if it is readily producible in that form and format. When the PHI is not readily producible in the electronic form and format requested, then the covered entity must provide access to an agreed upon alternative readable electronic format. See 45 CFR 164.524(c)(2)(ii). This means that, while a covered entity is not required to purchase new software or equipment in order to accommodate every possible individual request, the covered entity must have the capability to provide some form of electronic copy of PHI maintained electronically. It is only if the individual declines to accept any of the electronic formats readily producible by the covered entity that the covered entity may satisfy the request for access by providing the individual with a readable hard copy of the PHI.

The covered entity also may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided in addition to that PHI, so long as the individual in advance: (1) chooses to receive the summary or explanation (including in the electronic or paper form being offered by the covered entity); and (2) agrees to any fees (as explained below in the Section describing permissible Fees for Copies) that may be charged by the covered entity for the summary or explanation. See 45 CFR 164.524(c)(2)(iii).

A covered entity also must provide access in the manner requested by the individual, which includes arranging with the individual for a convenient time and place to pick up a copy of the PHI or to inspect the PHI (if that is the manner of access requested by the individual), or to have a copy of the PHI mailed or e-mailed, or otherwise transferred or transmitted to the individual to the extent the copy would be readily producible in such a manner. Whether a particular mode of transmission or transfer is readily producible will be based on the capabilities of the covered entity and the level of security risk that the mode of transmission or transfer may introduce to the PHI on the covered entity's systems (as opposed to security risks to the PHI once it has left the systems). A covered entity is not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access; whether the individual's requested mode of transfer or transmission presents such an unacceptable level of risk will depend on the covered entity's Security Rule risk analysis. See 45 CFR 164.524(c)(2) and (3), and 164.308(a)(1). However, mail and e-mail are generally considered readily producible by all covered entities. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail (except in the limited case where e-mail cannot accommodate the file size of requested images), and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI while in transit (such as where an individual has requested to receive her PHI by, and accepted the risks associated with, unencrypted e-mail). Thus, a covered entity may not require that an individual travel to the covered entity's physical location to pick up a copy of her PHI if the individual requests that the copy be mailed or e-mailed.

Timeliness in Providing Access

In providing access to the individual, a covered entity must provide access to the PHI requested, in whole, or in part (if certain access may be denied as explained below), no later than 30 calendar days from receiving the individual's request. See 45 CFR 164.524(b)(2). The 30 calendar days is an outer limit and covered entities are encouraged to respond as soon as possible. Indeed, a covered entity may have the capacity to provide individuals with almost instantaneous or very prompt electronic access to the PHI requested through personal health records, web portals, or similar electronic means. Further, individuals may reasonably expect a covered entity to be able to respond in a much faster timeframe when the covered entity is using health information technology in its day to day operations.

If a covered entity is unable to provide access within 30 calendar days -- for example, where the information is archived offsite and not readily accessible -- the covered entity may extend the time by no more than an additional 30 days. To extend the time, the covered entity must, within the initial 30 days, inform the individual in writing of the reasons for the delay and the date by which the covered entity will provide access. Only one extension is permitted per access request.

Fees for Copies

The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual. See 45 CFR 164.524(c)(4). The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law.

Denial of Access

Grounds for Denial

Under certain limited circumstances, a covered entity may deny an individual's request for access to all or a portion of the PHI requested. In some of these circumstances, an individual has a right to have the denial reviewed by a licensed health care professional designated by the covered entity who did not participate in the original decision to deny.

Unreviewable grounds for denial (45 CFR 164.524(a)(2)):

- The request is for psychotherapy notes, or information compiled in reasonable anticipation of, or for use in, a legal proceeding.
- An inmate requests a copy of her PHI held by a covered entity that is a correctional institution, or health care provider acting under the direction of the institution, and providing the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of correctional officers, employees, or other person at the institution or responsible for the transporting of the inmate. However, in these cases, an inmate retains the right to inspect her PHI.
- The requested PHI is in a designated record set that is part of a research study that includes treatment (e.g., clinical trial) and is still in progress, provided the individual agreed to the temporary suspension of access when consenting to participate in the research. The individual's right of access is reinstated upon completion of the research.
- The requested PHI is in Privacy Act protected records (i.e., certain records under the control of

a federal agency, which may be maintained by a federal agency or a contractor to a federal agency), if the denial of access is consistent with the requirements of the Act.

- The requested PHI was obtained by someone other than a health care provider (e.g., a family member of the individual) under a 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)). A licensed health care professional has determined in the exercise of professional judgment that:

- The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).
- The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
- The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person.

Note that a covered entity may not require an individual to provide a reason for requesting access, and the individual's rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is not a permitted reason to deny access. In addition, a covered entity may not deny access because a business associate of the covered entity, rather than the covered entity itself, maintains the PHI requested by the individual (e.g., the PHI is maintained by the covered entity's electronic health record vendor or is maintained by a records storage company offsite).

Carrying Out the Denial

If the covered entity denies access, in whole or in part, to PHI requested by the individual, the covered entity must provide a denial in writing to the individual no later than within 30 calendar days of the request (or no later than within 60 calendar days if the covered entity notified the individual of an extension). See 45 CFR 164.524(b)(2). The denial must be in plain language and describe the basis for denial; if applicable, the individual's right to have the decision reviewed and how to request such a review; and how the individual may submit a complaint to the covered entity or the HHS Office for Civil Rights. See 45 CFR 164.524(d).

If the covered entity (or one of its business associates) does not maintain the PHI requested, but knows where the information is maintained, the covered entity must inform the individual where to direct the request for access. See 45 CFR 164.524(d)(3).

The covered entity must, to the extent possible and within the above timeframes, provide the individual with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access. See 45 CFR 164.524(d)(1). Complexity in segregating the PHI does not excuse the obligation to provide access to the PHI to which the ground for denial does not apply.

Review of Denial

If the denial was based on a reviewable ground for denial and the individual requests review, the covered entity must promptly refer the request to the designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether to reaffirm or reverse the denial. The covered entity must then promptly provide written notice to the individual of the determination of the reviewing official, as well as take other action as necessary to carry out the determination. See 45 CFR 164.524(d)(4).

Individual's Right to Direct the PHI to Another Person

An individual also has a right to direct the covered entity to transmit the PHI about the individual directly to another person or entity designated by the individual. The individual's request to direct the PHI to another person must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI. A covered entity may accept an electronic copy of a signed request (e.g., PDF), as well as an electronically executed request (e.g., via a secure web portal) that includes an electronic signature. The same requirements for providing the PHI to the individual, such as the fee limitations and requirements for providing the PHI in the form and format and manner requested by the individual, apply when an individual directs that the PHI be sent to another person. See 45 CFR 164.524(c)(3).

State Laws

State laws that provide individuals with greater rights of access to their PHI than the Privacy Rule, or that are not contrary to the Privacy Rule, are not preempted by HIPAA and thus still apply. For example, a covered entity subject to a State law that requires that access to PHI be provided to an individual in a shorter time frame than that required in the Privacy Rule must provide such access within the shorter time frame because the State law is not contrary to the Privacy Rule.

Unless an exemption exists in the HIPAA Rules, State laws that are contrary to the Privacy Rule access provisions – such as those that prohibit certain laboratories from disclosing test reports directly to an individual – are preempted by HIPAA. See 45 CFR 160.203. Thus, these State laws do not apply when an individual exercises her HIPAA right of access. See 45 CFR Part 160, Subpart B.

Questions and Answers About HIPAA's Access Right

Scope of Information Covered by Access Right

What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans?

With limited exceptions, the HIPAA Privacy Rule gives individuals the right to access, upon request, the medical and health information (protected health information or PHI) about them in one or more designated record sets maintained by or for the individuals' health care providers and health plans (HIPAA covered entities). See 45 CFR 164.524. Designated record sets include medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals. See 45 CFR 164.501. Thus, individuals have a right to access a broad array of health information about themselves, whether maintained by a covered entity or by a business associate on the covered entity's behalf, including medical records, billing and payment records, insurance information, clinical laboratory test reports, X-rays, wellness and disease management program information, and notes (such as clinical case notes or "SOAP" notes (a method of making notes in a patient's chart) but not including psychotherapy notes as explained below), among other information generated from treating the individual or paying for the individual's care or otherwise used to make decisions about individuals. In responding to a request for access, a covered entity is not, however, required to create new information, such as explanatory materials or analyses, that does not already exist in the designated record set. Further, while individuals have a right to a broad array of PHI about themselves in a designated record set, a covered entity is only required to provide access to the PHI to which the individual requests access.

Individuals do not have a right to access PHI about them that is not part of a designated record set because this information is not used to make decisions about individuals. This may include certain quality assessment or improvement records, patient safety activity records, or business planning, development, and management records that are used for business decisions more generally rather than to make decisions about individuals. For example, peer review files, practitioner or provider performance evaluations, quality control records used to improve customer service, and formulary development records may be generated from and include an individual's PHI but may not be in the covered entity's designated record set(s) to which the individual has access. However, the underlying PHI from the individual's medical or payment records used to generate such information remains part of the designated record set

and subject to access by the individual. For example, an individual would not have the right to access internal memos related to the development of a formulary; however, an individual does have the right to access information about prescription drugs that were prescribed for her, and claims records related to payment for those drugs, even if that information was relied on in, or helped inform, the development of the formulary.

Individuals also do not have a right to access the psychotherapy notes that a mental health professional maintains separately from the individual's medical record and that document or analyze the contents of a counseling session with the individual. In addition, individuals do not have a right to access information about the individual compiled in reasonable anticipation of, or for use in, a legal proceeding (but the individual retains the right to access the underlying PHI from the designated record set(s) about the individual used to generate the litigation information). However, a covered entity has the discretion to share this information with the individual if it chooses. See 45 CFR 164.524(a)(1) – (a)(3) for a complete list of exceptions to the right of access.

Does an individual's right under HIPAA to access their health information apply only to the information a health care provider maintains about the individual in an Electronic Health Record (EHR), or paper medical record?

No. An individual has a broad right under the HIPAA Privacy Rule to access the PHI about the individual in all designated record sets maintained by or for a covered entity, whether in electronic or paper form, not just the designated record set that comprises the "medical record." See 45 CFR 164.524(a). (However, if the same PHI is maintained in more than one designated record set, a covered entity need only produce the information once in response to a request for access.) A designated record set also includes billing and payment records, claims and insurance information, as well as other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals. See the definition of "designated record set" at 45 CFR 164.501.

Does the individual have a right to access PHI about themselves maintained by a covered entity that is very old or is archived?

Yes. An individual has a right to access PHI about themselves in a medical record or other designated record set maintained by a covered entity, regardless of the date the information was created or whether the information is maintained onsite, remotely, or is archived. There are only very limited grounds under which a covered entity may deny an individual access to PHI about herself in a designated record set, which do not include the age or location of the information. See 45 CFR 164.524(a)(2) – (a)(3).

Does an individual have a right to access all of the information a covered entity maintains in the individual's medical record?

Yes. Except in very limited circumstances, an individual has a right to access all PHI about the individual that a covered entity (or its business associate) maintains in one or more designated record sets. A designated record set is defined to include the medical record about the individual. Thus, an individual

generally has a right to access all of the information about the individual that a covered entity maintains in the individual's medical record, including information the individual provided to the covered entity herself, as well as PHI about the individual contributed to the record by other health care providers or covered entities. See 45 CFR 164.524(a)(2) – (a)(3) for the limited grounds upon which a covered entity may deny an individual access to PHI in a designated record set.

Under what circumstances may a covered entity deny an individual's request for access to the individual's PHI?

A covered entity may deny an individual access to all or a portion of the PHI requested in only very limited circumstances. For example, a covered entity may deny an individual access if the information requested is not part of a designated record set maintained by the covered entity (or by a business associate for a covered entity), or the information is excepted from the right of access because it is psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a legal proceeding (but the individual retains the right to access the underlying PHI from the designated record set(s) about the individual used to generate this information).

Another limited ground for denial exists if a licensed health care professional determines in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. For example, a covered entity may deny a suicidal patient access to information that a provider determines in his professional judgment is reasonably likely to lead the patient to take her own life. However, we stress that this ground is narrowly construed in order to protect individuals' autonomy interests and their right under the Privacy Rule to obtain information about themselves, which is fundamental in facilitating individuals' active participation in their own health care. General concerns about psychological or emotional harm are not sufficient to deny an individual access (e.g., concerns that the individual will not be able to understand the information or may be upset by it). In addition, the requested access must be reasonably likely to cause harm or endanger physical life or safety. Thus, concerns based on the mere possibility of harm are not sufficient to deny access. As a result, we expect this ground for denial to apply in extremely rare circumstances. Further, an individual who is denied access based on these grounds has a right to have the denial reviewed by a licensed health care professional designated by the covered entity as a reviewing official who did not participate in the original decision to deny access.

For a complete list of the grounds and conditions for denial of access, see 45 CFR 164.524(a)(2)-(4). Note that an individual may not be required to provide a reason for requesting access, and the individual's rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is not a permitted reason to deny access.

If a covered entity denies access, in whole or in part, to PHI requested by the individual based on one or more permitted grounds, the covered entity must provide a denial in writing to the individual no later than 30 calendar days after the request (or no more than 60 calendar days if the covered entity notified the individual of an extension). See 45 CFR 164.524(b)(2). The denial must be in plain language and describe the basis for denial; if applicable, the individual's right to have the decision reviewed and how to request such a review; and how the individual may submit a complaint to the covered entity or the HHS Office for Civil Rights. See 45 CFR 164.524(d).

The covered entity must, to the extent possible, provide the individual with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access. See 45 CFR 164.524(d)(1).

Does an individual have a right under HIPAA to access PHI about the individual maintained by a business associate of a covered entity?

Yes. An individual's right under the HIPAA Privacy Rule to access PHI about themselves extends to PHI in a designated record set maintained by a business associate on behalf of a covered entity. Thus, if an individual submits a request for access to PHI, the covered entity is responsible for providing the individual with access not only to the PHI it holds but also to the PHI held by one or more of its business associates. However, if the same PHI that is the subject of an access request is maintained in both the designated record set of the covered entity and the designated record set of the business associate, the PHI need only be produced once in response to the request for access. See 45 CFR 164.524(c)(1).

With respect to PHI in a designated record set maintained by a business associate, the business associate agreement between the covered entity and the business associate will govern whether the business associate will provide access directly to the individual or will provide the PHI that is the subject of the individual's access request to the covered entity for the covered entity to then provide access to the individual. However, regardless of how and to what extent a business associate supports or fulfills a covered entity's obligation to provide access to an individual, a request for access still must be acted upon within 30 calendar days (or 60 calendar days if an extension is applicable) of receipt of the request by either the covered entity, or by a business associate if the request was made directly to the business associate because the covered entity instructed individuals through its notice of privacy practices (or otherwise) to submit access requests directly to the business associate. Further, all of the access requirements that apply with respect to PHI held by the covered entity (e.g., limitations on fees that may be charged) apply with respect to PHI held by the business associate.

Does an individual have a right under HIPAA to access from a clinical laboratory the genomic information the laboratory has generated about the individual?

Yes. An individual has a right under the HIPAA Privacy Rule to access, upon request, PHI about the individual in a designated record set maintained by or for a clinical laboratory that is a covered entity. The designated record set includes not only the laboratory test reports but also the underlying information generated as part of the test, as well as other information concerning tests a laboratory runs on an individual. For example, 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.

Does an individual have a right under HIPAA to access more than just test results from a clinical laboratory?

Yes. Under the HIPAA Privacy Rule, an individual has a general right to access, upon request, PHI about the individual in a designated record set maintained by or for a clinical laboratory that is a covered entity. A test result or test report is only part of the designated record set a clinical laboratory may hold. To the extent an individual requests access to all of her information held by the laboratory, the laboratory is required to provide access to all of the PHI about the individual in its designated record set. This could include, for example, completed test reports and the underlying data used to generate the reports, test orders, ordering provider information, billing information, and insurance information.

Timelines for Providing Access

How timely must a covered entity be in responding to individuals' requests for access to their PHI?

Under the HIPAA Privacy Rule, a covered entity must act on an individual's request for access no later than 30 calendar days after receipt of the request. If the covered entity is not able to act within this timeframe, the entity may have up to an additional 30 calendar days, as long as it provides the individual – within that initial 30-day period – with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request. See 45 CFR 164.524(b)(2).

These timelines apply regardless of whether:

- The PHI that is the subject of the request is maintained by the covered entity or by a business associate on behalf of the covered entity, or the covered entity uses a business associate to fulfill individual requests for access. The 30-day clock starts on the date that the covered entity receives a request for access, so any delay in obtaining the necessary information from a business associate or forwarding the request to the business associate for action "uses up" part of the allotted time. Alternatively, the 30-day clock starts when, instead of the covered entity, a business associate receives a request directly from an individual because the covered entity instructed the individual through its notice of privacy

practices (or otherwise) to submit the access request directly to its business associate for processing.

- The covered entity negotiates with the individual on the format of the response. Covered entities that spend significant time before reaching agreement with individuals on format are depleting the 30 days allotted for the response by that amount of time.
- The PHI that is the subject of the request is old, archived, and/or not otherwise readily accessible.

These timelines are outer limits, and it is expected that many covered entities should be able to respond to requests for access well before these outer limits are reached. However, in cases where a covered entity is aware that an access request may take close to these outer time limits to fulfill, the entity is encouraged to provide the requested information in pieces as it becomes available, if the individual indicates a desire to receive the information in such a manner.

Under the EHR Incentive Program, participating providers are required to provide individuals with access to certain information on much faster timeframes (e.g., a discharge summary within 36 hours of discharge, a lab result within 4 business days after the provider has received the results) than under HIPAA. How do these requirements operate together?

Health care providers participating in the EHR Incentive Program may use the patient engagement tools of their Certified EHR Technology to make certain information available to patients quickly and satisfy their EHR Incentive Program objectives. Doing so also has the added benefit of satisfying an individual's request for access under HIPAA, where the PHI requested by the individual is available through the Certified EHR Technology, and the individual agrees to access the information in this way. While the Privacy Rule permits a covered entity to take up to 30 calendar days from receipt of a request to provide access (with one extension for up to an additional 30 calendar days when necessary), covered entities are strongly encouraged to provide individuals with access to their health information much sooner, and to take advantage of technologies that enable individuals to have faster or even immediate access to the information.

Why does HIPAA give covered entities 30 days to respond to individuals' requests for access to their PHI? In the digital age, allowing covered entities 30 days to provide individuals with access to their health information seems too long; individuals need this information promptly to manage their health and health care.

While some individual access requests should be fairly easy to fulfill (e.g., those that can be satisfied through the use of Certified EHR Technology), the HIPAA Privacy Rule recognizes that there may be other circumstances where additional time and effort may be necessary to locate and obtain the PHI that is the subject of the request, or to provide the PHI in the format requested or agreed to by the individual, or otherwise to act on the request. The Privacy Rule is intended to set the outer time limit for providing access, not indicate the desired or best result, and it is expected that many covered entities should be able to respond to requests for access well before the 30 day outer limit. Further, as technology evolves

and PHI becomes more readily available via easy-to-use digital technologies, the ability to provide very prompt or almost instantaneous access to individuals will increase. The Department will continue to monitor these developments.

In some cases, the 30-day timeframe from a request to provide an individual with access to her PHI may not be sufficient time for a clinical laboratory to complete the test report that is the subject of the individual's request. What can a clinical laboratory do in these cases?

In those limited cases where, due to the nature of the test and the timing of the individual's request, 30 calendar days may not be sufficient to complete a test report to which the individual has requested access, the laboratory may notify the individual in writing within the 30-day period of the need and specific reason for the delay in providing access to the completed test result and the date by which the laboratory will complete its action on the request, in accordance with § 164.524(b)(2)(iii) of the HIPAA Privacy Rule. The Privacy Rule allows only one extension on an access request and the extension may not exceed an additional 30 calendar days. In the rare circumstance where 60 calendar days is not sufficient to provide the individual with access to the completed test report requested by the individual, the covered laboratory may, at the end of the 60 day period, satisfy the access request by providing the individual with access to the PHI that does exist at the time (e.g., test requisitions, the underlying data being used to generate the reports, other completed test reports) in the designated record set.

However, to avoid this situation to the extent possible, in cases where the laboratory knows that a particular test report will take longer than the HIPAA access timeframes, we expect the laboratory to explain this circumstance to the individual. Upon informing individuals of this situation when they request access, the individuals may be willing to withdraw or hold their request until a later time to ensure that they get access to what they want or need. If an individual chooses not to withdraw his or her request for access, the individual will then have a right only to obtain the PHI in the designated record set at the time the request is fulfilled, which may not include the particular test report requested because it is not yet complete.

Form and Format and Manner of Access

Under the HIPAA Privacy Rule, do individuals have the right to an electronic copy of their PHI?

Yes, in most cases. If the PHI is maintained by a covered entity electronically, an individual has a right to receive an electronic copy of the information upon request (assuming the covered entity does not have a ground for denial under 45 CFR 164.524(a)(2) or (a)(3)). The covered entity must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in that form and format, or if not, in a readable alternative electronic format as agreed to by the individual and covered entity. See 45 CFR 164.524(c)(2)(ii). Where an individual requests access to PHI

that is maintained electronically by a covered entity, the covered entity may provide the individual with a paper copy of the PHI to satisfy the request only in cases where the individual declines to accept any of the electronic formats readily producible by the covered entity.

If the individual requests an electronic copy of PHI that the covered entity maintains only on paper, the covered entity must provide the individual with the electronic copy if the copy is readily producible electronically (e.g., the covered entity can readily scan the paper record into an electronic format) and in the electronic format requested if readily producible in that format, or if not, in a readable alternative electronic format as agreed to by the covered entity and individual. If the copy is not readily producible in electronic form, or the individual declines to accept the electronic format(s) readily producible by the covered entity, then a readable hard copy of the PHI may be provided to satisfy the access request. See 45 CFR 164.524(c)(2)(i).

If an individual requests an electronic copy of the individual's PHI that the covered entity maintains only on paper, is the covered entity required to scan the paper records to create an electronic copy of the PHI for the individual?

While a covered entity is not required to purchase a scanner to create electronic copies, if a covered entity can readily produce an electronic copy of the PHI for the individual by scanning the records, it must do so. In particular, if an individual requests an electronic copy of PHI in a specific format, and a covered entity maintains that PHI only on paper, the covered entity must provide the individual with the electronic copy, in the format requested, if the copy is readily producible electronically and readily producible in the electronic format requested. If the copy is readily producible electronically but not in the specific format requested, the covered entity may offer the individual the copy in an alternative readable electronic format. If the copy is not readily producible in electronic form, or the individual declines to accept the electronic format(s) that are readily producible by the covered entity, then the covered entity may provide the individual with a readable hard copy of the PHI to satisfy the access request. See § 164.524(c)(2)(i). For example, a covered entity that maintains the requested PHI only on paper may be able to readily produce a scanned PDF version of the PHI but not the requested Word version. In this case, the covered entity may provide the individual with the PDF version if the individual agrees to accept the PDF version. If the individual declines to accept the PDF version, or if the covered entity is not able to readily produce a PDF or other electronic version of the PHI, the covered entity may provide the individual with a hard copy, such as a photocopy, of the PHI.

When an individual exercises her HIPAA right to get an electronic copy of her PHI, can the individual choose the electronic format of the copy?

While individuals do not have an unlimited choice in the form of electronic copy requested, and covered entities are not required to purchase new software or other equipment in order to accommodate every possible individual request, the individual does have a right to receive the copy in the form and format requested by the individual if the copy is readily producible in that form and format. For example, an

individual may request that an electronic copy of her PHI be provided to her in Microsoft (MS) Word; MS Excel; Portable Document Format (PDF); or as structured, machine readable data (e.g., a document following the Consolidated Clinical Document Architecture (CCDA) standard using LOINC (to represent lab tests) and RxNorm (to represent medications)); or other electronic format; and the covered entity must provide the copy in the requested format if readily producible in that format. Further, if the PHI that is the subject of the request is maintained electronically by a covered entity, the entity is required to have the capability to provide some form of electronic copy (see 78 FR 5633, https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf) – and this means that some covered entities may need to make some investments (which cannot be charged to individuals) in order to meet this baseline requirement. If an individual requests a form of electronic copy that the covered entity is unable to produce, the covered entity must offer other electronic formats that are available on its systems. If the individual declines to accept any of the electronic formats that are readily producible by the covered entity, only then may the covered entity provide a hard copy to fulfill the access request. Thus, individuals who request electronic access to PHI maintained electronically can be diverted to receiving a paper copy only in circumstances where all of the covered entities' existing capabilities for readily producing electronic copies have been presented to the individual but the individual has determined that those formats are not acceptable to her.

When an individual requests access to PHI in a particular form or format, the question for the covered entity is whether or not the entity is able to readily produce the copy in that format – which is a matter of capability, not "willingness." Thus, if a covered entity has the capability to readily produce the requested format, it is not permissible for the covered entity to deny the individual access to that format because the entity would prefer that the individual receive a different format, or utilize other customary record access processes of the entity.

What is the intersection of the HIPAA right of access and the HITECH Act's Medicare and Medicaid Electronic Health Record Incentive Program's "View, Download, and Transmit" provisions?

Under the HIPAA Privacy Rule, an individual has the right to access PHI maintained about the individual by a covered entity in a designated record set. This may contain electronic or non-electronic PHI. See 45 CFR 164.524(a)(1). Under the HITECH Act's Electronic Health Record (EHR) Incentive Program, eligible professionals, eligible hospitals, and critical access hospitals (CAHs) may receive incentive payments under Medicare and Medicaid and avoid payment reductions under Medicare for successfully demonstrating meaningful use of Certified EHR Technology, which includes providing patients the ability to view online, download, and transmit their health information. It is important to note that in some respects the EHR Incentive Program contains more exacting standards than the baseline requirements of the HIPAA Privacy Rule, while the HIPAA Privacy Rule contains more comprehensive requirements than the EHR Incentive Program (e.g., the HIPAA Privacy Rule access right applies to electronic and paper records, while the EHR Incentive Program applies to certain electronic records).

Below are some key distinctions between the HIPAA right of access and the individual access opportunities that may be offered through the EHR Incentive Program:

EHR Incentive Program	**HIPAA Privacy Rule**
Professional or hospital proactively makes available certain information for the patient to view, download, or transmit (more than 50% of patients are provided timely access in Stage 2; more than 80% in Stage 3)	Covered entity required by law to provide individuals with access upon request
Access is to a specific set of data (e.g., recent lab test results, current medication list and medication history, problem list)* maintained in Certified EHR Technology (for Stage 3, the specific set of data is known as the Common Clinical Data Set (CCDS), as defined in the 2015 Edition Health IT Certification Rule**) *See the EHR Incentive Program Final Rule at 80 FR 62812, https://www.federalregister.gov/articles/2015/10/16/2015-25595/medicare-and-medicaid-programs-electronic-health-record-incentive-program-stage-3-and-modifications **See 80 FR 62602, https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base	Access is to requested PHI that is in a designated record set which is PHI that is either maintained electronically (e.g., in the EHR) or other medical information that is not stored in the EHR (e.g., PHI that is stored on paper, billing records, and other records used to make decisions about individuals)
Access must be timely provided (e.g., in Stage 2, professionals must make information available within 4 business days of its availability to the professional, and hospitals must make information about hospital stays available within 36 hours of discharge; for Stage 3, information must be available to the patient within 48 hours of its availability to a professional and 36 hours of its availability to a hospital)	Prompt access is encouraged but covered entities may take no longer than 30 days from receipt to act on a request for access (and may take another 30 days to respond if the individual is notified in writing of the reason for delay during the initial 30 day period)

Administered by the Centers for Medicare & Medicaid Services (with respect to the EHR Incentive Program) and the Office of the National Coordinator for Health IT (with respect to the Health IT Certification Program)	Administered by the HHS Office for Civil Rights

Although the EHR Incentive Program and the HIPAA Privacy Rule are distinct, it is possible for a provider or hospital to leverage its Certified EHR Technology to fulfill its HIPAA Privacy Rule obligations with respect to individual access in circumstances where the individual either: (1) requests access to PHI that is held in the Certified EHR Technology; or (2) requests access to his PHI, the covered entity professional or hospital informs the individual that the PHI requested is available through the Certified EHR Technology, and the individual agrees to access the requested PHI through the Certified EHR Technology.

In scenario 1, the individual is aware of the EHR Incentive Program and specifically requests access to her PHI via the functionality of the Certified EHR Technology. For example, in exercising her right of access under the HIPAA Privacy Rule, an individual could request a copy of her information that constitutes the CCDS through the provider's Certified EHR Technology portal or that it be sent from the Certified EHR Technology to the individual's Direct address (an electronic address for securely exchanging health information using the Direct technical standard). If the provider is using Certified EHR Technology, the HIPAA Privacy Rule requires the provider to grant this request from the individual because the form and format requested is "readily producible" using the provider's Certified EHR Technology. At the same time, the provider should be able to count this access by the individual for purposes of meeting its EHR Incentive Program objectives, as long as the access was provided within the timeframes required by the EHR Incentive Program. Because the Privacy Rule provides up to 30 days to act on an access request, meeting the more prompt deadlines of the EHR Incentive Program clearly complies with the Privacy Rule's deadlines.

In scenario 2, the individual has requested a copy of certain of his PHI, and the provider recognizes that the PHI requested by the individual would be easily available through the Certified EHR Technology. The individual asks for the information in PDF format; the provider instead offers to set up an account for the individual so that the individual can access this information directly through the portal in the Certified EHR Technology. If the individual agrees to the portal access, the provider will be able to satisfy the individual's HIPAA access request using the Certified EHR Technology portal, while at the same time being able to count the access for purposes of meeting EHR Incentive Program objectives (as long as the access was provided within the timeframes required by the EHR Incentive Program). If the individual declines the

offer and instead maintains his request to receive a copy of his PHI in PDF format, the HIPAA Privacy Rule requires the provider to provide the individual with a copy in PDF format, if the PHI is readily producible in that format or, if not, in an alternative electronic format that is agreeable to the patient. Further, the individual at all times retains the right to access his PHI in a designated record set that is not part of or available through the Certified EHR Technology.

Does an individual have a right under HIPAA to access his PHI in a particular technical standard?

In some circumstances, an individual may request access to an electronic copy of his PHI in a particular technical standard – for example, a copy of the individual's medication data represented in RxNorm or a lab test represented in LOINC. An individual may request PHI in a particular standard in order to use that information in other software the individual is using. If the covered entity is able to readily produce the PHI in the requested standard format, the covered entity must do so (unless the entity has a ground for denial as specified in the Privacy Rule at 45 CFR 164.524(a). (We note that individuals, in exercising their rights of access under the Privacy Rule, are not required to state their purpose for requesting access, regardless of whether or not a particular form or format for the request is specified, and an individual's rationale for requesting access is not a reason to deny access.)

Do individuals have a right under HIPAA to get copies of their x-rays or other diagnostic images, and if so, in what format?

Yes. An individual has a right to receive PHI about the individual maintained by a covered entity in a designated record set, such as a medical record. See 45 CFR 164.524(a)(1). This includes x-rays or other images in the record. As with other PHI in a designated record set, the individual has a right to access the information in the form and format she requests, as long as the covered entity can readily produce it in that form and format. See 45 CFR 164.524(c). The large file size of some x-rays or other images may impact the mechanism for access (e.g., the format agreed upon by the individual and the covered entity must accommodate the file size).

Do individuals have the right under HIPAA to have copies of their PHI transferred or transmitted to them in the manner they request, even if the requested mode of transfer or transmission is unsecure?

Yes, as long as the PHI is "readily producible" in the manner requested, based on the capabilities of the covered entity and transmission or transfer in such a manner would not present an unacceptable level of security risk to the PHI on the covered entity's systems, such as risks that may be presented by connecting an outside system, application, or device directly to a covered entity's systems (as opposed to security risks to PHI once it has left the systems). For example, individuals generally have a right to receive copies of their PHI by mail or e-mail, if they request. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI once it has left the systems. Thus, a covered entity may not require that an individual travel to the

covered entity's physical location to pick up a copy of her PHI if the individual requests the copy be mailed or e-mailed. In the limited case where a covered entity is unable to e-mail the PHI as requested, such as in the case where diagnostic images are requested and e-mail cannot accommodate the file size of the images, the covered entity should offer the individual alternative means of receiving the PHI, such as on portable media that can be mailed to the individual.

Further, while covered entities are required by the Privacy and Security Rules to implement reasonable safeguards to protect PHI while in transit, individuals have a right to receive a copy of their PHI by unencrypted e-mail if the individual requests access in this manner. In such cases, the covered entity must provide a brief warning to the individual that there is some level of risk that the individual's PHI could be read or otherwise accessed by a third party while in transit, and confirm that the individual still wants to receive her PHI by unencrypted e-mail. If the individual says yes, the covered entity must comply with the request. We note that providers using the 2015 edition of Certified EHR Technology will have the capability to send unencrypted e-mail transmissions directly from that technology.

Whether an individual has a right to receive a copy of her PHI through other unsecure modes of transmission or transfer (assuming the individual requests the mode and accepts the risk) depends on the extent to which the mode of transmission or transfer is within the capabilities of the covered entity and the mode would not present an unacceptable level of risk to the security of the PHI on the covered entity's systems (as explained above), based on the covered entity's Security Rule risk analysis. For example, a covered entity's risk analysis may provide that connecting an outside (foreign) device, such as a USB drive, directly to the entity's systems presents an unacceptable level of risk to the PHI on the systems. In this case, the covered entity is not required to agree to an individual's request to transfer the PHI in this manner, but the entity must offer some other means of providing electronic access to the PHI.

Note that while an individual can receive copies of her PHI by unsecure methods if that is her preference, as described in more detail above, a covered entity is not permitted to require an individual to accept unsecure methods of transmission in order to receive copies of her health information.

Is a covered entity responsible if it complies with an individual's access request to receive PHI in an unsecure manner (e.g., unencrypted e-mail) and the information is intercepted while in transit?

No. While covered entities are responsible for adopting reasonable safeguards in implementing the individual's request (e.g., correctly entering the e-mail address), covered entities are not responsible for a disclosure of PHI while in transmission to the individual based on the individual's access request to receive the PHI in an unsecure manner (assuming the individual was warned of and accepted the risks associated with the unsecure transmission). This includes breach notification obligations and liability for disclosures that occur in transit. Further, covered entities are not responsible for safeguarding the

information once delivered to the individual. Covered entities are responsible for breach notification for unsecured transmissions and may be liable for impermissible disclosures of PHI that occur in all contexts except when fulfilling an individual's right of access under 45 CFR 164.524 to receive his or her PHI or direct the PHI to a third party in an unsecure manner.

Do individuals have a right under HIPAA to have their PHI downloaded on portable media that they provide?

Whether PHI is "readily producible" for purposes of providing access will depend on the extent to which the requested method of copying, transfer, or transmission is within the capabilities of the covered entity and would not present an unacceptable level of risk to the security of the PHI on the covered entity's systems, based on the covered entity's Security Rule risk analysis.

With respect to portable media supplied by an individual, covered entities are required by the Security Rule to perform a risk analysis related to the potential use of external portable media and are not required to accept the external media if they determine there is an unacceptable level of risk to the PHI on their systems. However, covered entities are not then permitted to require individuals to purchase a portable media device from the covered entity if the individual does not wish to do so. The individual may in such cases opt to receive an alternative form of the electronic copy of the PHI, such as through email.

Do individuals have a right under HIPAA to have a covered entity establish a direct connection between the covered entity's system and the individual's app or device in order to provide the individuals with access to their PHI?

Whether PHI is "readily producible" for purposes of providing access will depend on the extent to which establishing the connection is within the capabilities of the covered entity and would not present an unacceptable level of risk to the security of the PHI on a covered entity's systems, based on the covered entity's Security Rule risk analysis.

A covered entity may determine that it has the capability to establish the type of connection requested in a manner consistent with the applicable security measures implemented in accordance with its security management process. In that case, the covered entity must provide access in the manner requested by the individual. Further, we note that starting in 2018, under Stage 3 of the EHR Incentive Program, eligible professionals, eligible hospitals, and critical access hospitals (CAHs) using Certified EHR Technology must enable application programming interface (API) functionality that would allow patients to use the application of their choice to access their data. In addition, we note that many provider systems are already using API functionality to provide patients with access to their data today in a secure manner. We expect that covered entities will assess and address any security considerations associated with connecting their systems with individual applications or devices, including through Certified EHR Technology (where applicable), as part of their HIPAA security management process.

Does an individual have a right under HIPAA to access their health information in human readable form?

Yes. In general, a covered entity must provide an individual with access to PHI about the individual in a designated record set in the form and format requested by the individual, if it is readily producible in such form and format. In cases where the PHI is not readily producible in the requested form and format, the covered entity must provide the PHI in a *readable* alternative form and format as agreed to by the covered entity and the individual. See 45 CFR 164.524(c)(2). Thus, individuals have a right under HIPAA to access PHI about themselves in human readable form. In cases where a covered entity is providing an individual with an electronic copy of PHI, we also expect the covered entity to provide the copy in machine readable form (i.e., in a form able to be processed by a computer), to the extent possible and where consistent with the individual's request.

Other Questions on Access Right

Is a health care provider permitted to deny an individual's request for access because the individual has not paid for health care services provided to the individual?

No. A covered entity may charge an individual that has requested a copy of her PHI a reasonable, cost-based fee for the copy. See 45 CFR 164.524(c)(4). However, a covered entity may not withhold or deny an individual access to her PHI on the grounds that the individual has not paid the bill for health care services the covered entity provided to the individual.

If an individual's physician orders a test from a clinical laboratory that may take multiple steps or a series of tests to complete, at what point does the test report become part of the laboratory's designated record set to which an individual has a right of access?

For purposes of the HIPAA Privacy Rule, clinical laboratory test reports become part of the laboratory's designated record set when they are "complete," which means that all results associated with an ordered test are finalized and ready for release.

Is a clinical laboratory required to provide an individual with access to a test report that is not yet complete?

No. For purposes of the HIPAA Privacy Rule, clinical laboratory test reports become part of the laboratory's designated record set when they are "complete," which means that all results associated with an ordered test are finalized and ready for release. However, other information concerning the test may be part of the designated record set and thus, accessible to the individual, even if the test report has not yet been completed, such as test orders, ordering provider information, billing information, and insurance information.

If an individual requests access from a clinical laboratory to a test report on the individual, is the laboratory required to interpret the test results for the individual?

No. There is no requirement in the HIPAA Privacy Rule that clinical laboratories interpret test results for patients. An individual has a right under the HIPAA Privacy Rule merely to inspect or receive a copy (or direct the copy to a designated third party), upon request, of the completed test reports (as well as other information in the designated record set) maintained by a laboratory that is a covered entity. Laboratories

may continue to refer patients with questions about the test results back to their ordering or treating providers. However, while not required, a laboratory providing a test report to an individual that has requested access to the report may also provide educational or explanatory materials regarding the test results to individuals if it chooses to do so. Similarly, a laboratory that wishes to include a disclaimer, caveat, or other statement explaining the limitations of the laboratory data for diagnosis or treatment or other purposes may do so.

Frequently Asked Questions for Professionals - Please see the HIPAA FAQs for additional guidance on health information privacy topics.

Content created by Health Information Privacy Division