

Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524 Part 2

Fees That Can Be Charged to Individuals for Copies of their PHI

May a covered entity charge individuals a fee for providing the individuals with a copy of their PHI?

Yes, but only within specific limits. The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee to provide the individual (or the individual's personal representative) with a copy of the individual's PHI, or to direct the copy to a designated third party. The fee may include only the cost of certain labor, supplies, and postage:

1. Labor for copying the PHI requested by the individual, whether in paper or electronic form. Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied. Labor for copying does not include costs associated with reviewing the request for access; or searching for and retrieving the PHI, which includes locating and reviewing the PHI in the medical or other record, and segregating or otherwise preparing the PHI that is responsive to the request for copying.

While it has always been prohibited to pass on to an individual labor costs related to search and retrieval, our experience in administering and enforcing the HIPAA Privacy Rule has shown there is confusion about what constitutes a prohibited search and retrieval cost and this guidance further clarifies this issue. This clarification is important to ensure that the fees charged reflect only what the Department considers "copying" for purposes of applying 45 CFR 164.524(c)(4)(i) and do not impede individuals' ability to receive a copy of their records.

2. Supplies for creating the paper copy (e.g., paper, toner) or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media. However, a covered entity may not require an individual to purchase portable media; individuals have the right to have their PHI e-mailed or mailed to them upon request.
3. Labor to prepare an explanation or summary of the PHI, if the individual in advance both chooses to receive an explanation or summary and agrees to the fee that may be charged.
4. Postage, when the individual requests that the copy, or the summary or explanation, be mailed.

Thus, costs associated with updates to or maintenance of systems and data, capital for data storage and maintenance, labor associated with ensuring compliance with HIPAA (and other applicable law) in fulfilling the access request (e.g., verification, ensuring only information about the correct individual is included, etc.) and other costs not included above, even if authorized by State law, are not permitted for purposes of calculating the fees that can be charged to individuals. See 45 CFR 164.524(c)(4).

Further, while the Privacy Rule permits the limited fee described above, covered entities should provide individuals who request access to their information with copies of their PHI free of charge. While covered entities should forgo fees for all individuals, not charging fees

for access is particularly vital in cases where the financial situation of an individual requesting access would make it difficult or impossible for the individual to afford the fee. Providing individuals with access to their health information is a necessary component of delivering and paying for health care. We will continue to monitor whether the fees that are being charged to individuals are creating barriers to this access, will take enforcement action where necessary, and will reassess as necessary the provisions in the Privacy Rule that permit these fees to be charged.

What labor costs may a covered entity include in the fee that may be charged to individuals to provide them with a copy of their PHI?

A covered entity may include reasonable labor costs associated only with the: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; and (2) labor to prepare an explanation or summary of the PHI, if the individual in advance both chooses to receive an explanation or summary and agrees to the fee that may be charged.

Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied. For example, labor for copying may include labor associated with the following, as necessary to copy and deliver the PHI in the form and format and manner requested or agreed to by the individual:

- Photocopying paper PHI.
- Scanning paper PHI into an electronic format.
- Converting electronic information in one format to the format requested by or agreed to by the individual.
- Transferring (e.g., uploading, downloading, attaching, burning) electronic PHI from a covered entity's system to a web-based portal (where the PHI is not already maintained in or accessible through the portal), portable media, e-mail, app, personal health record, or other manner of delivery of the PHI.
- Creating and executing a mailing or e-mail with the responsive PHI.

While we allow labor costs for these limited activities, we note that as technology evolves and processes for converting and transferring files and formats become more automated, we expect labor costs to disappear or at least diminish in many cases.

In contrast, labor for copying does not include labor costs associated with:

- Reviewing the request for access.
- Searching for, retrieving, and otherwise preparing the responsive information for copying. This includes labor to locate the appropriate designated record sets about the individual, to review the records to identify the PHI that is responsive to the request and to ensure the information relates to the correct individual, and to segregate, collect, compile, and otherwise prepare the responsive information for copying.

May a covered health care provider charge a fee under HIPAA for individuals to access the PHI that is available through the provider's EHR technology that has been certified as being capable of making the PHI accessible?

No. The HIPAA Privacy Rule at 45 CFR 164.524(c)(4) permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual. Where an individual requests or agrees to access her PHI available through the View, Download, and Transmit functionality of the CEHRT, we believe there are no labor costs and no costs for supplies to enable such access. Thus, a covered health care provider cannot charge an individual a fee when it fulfills an individual's HIPAA access request using the View, Download, and Transmit functionality of the provider's CEHRT.

May a covered entity that uses a business associate to act on individual requests for access pass on the costs of outsourcing this function to individuals when they request copies of their PHI?

No. A covered entity may charge individuals a reasonable, cost-based fee that includes only labor for copying the PHI, costs for supplies, labor for creating a summary or explanation of the PHI if the individual requests a summary or explanation, and postage, if the PHI is to be mailed. See 45 CFR 164.524(c)(4). Administrative and other costs associated with outsourcing the function of responding to individual requests for access cannot be the basis for any fees charged to individuals for providing that access.

Must a covered entity inform individuals in advance of any fees that may be charged when the individuals request a copy of their PHI?

Yes. When an individual requests access to her PHI and the covered entity intends to charge the individual the limited fee permitted by the HIPAA Privacy Rule for providing the individual with a copy of her PHI, the covered entity must inform the individual in advance of the approximate fee that may be charged for the copy. An individual has a right to receive a copy of her PHI in the form and format and manner requested, if readily producible in that way, or as otherwise agreed to by the individual. Since the fee a covered entity is permitted to charge will vary based on the form and format and manner of access requested or agreed to by the individual, covered entities must, at the time such details are being negotiated or arranged, inform the individual of any associated fees that may impact the form and format and manner in which the individual requests or agrees to receive a copy of her PHI. The failure to provide advance notice is an unreasonable measure that may serve as a barrier to the right of access. Thus, this requirement is necessary for the right of access to operate consistent with the HIPAA Privacy Rule. Further, covered entities should post on their web sites or otherwise make available to individuals an approximate fee schedule for regular types of access requests. In addition, if an individual requests, covered entities should provide the individual with a breakdown of the charges for labor, supplies, and postage, if applicable, that make up the total fee charged. We note that this information would likely be requested in any action taken by OCR in enforcing the individual right of access, so entities will benefit from having this information readily available.

How can covered entities calculate the limited fee that can be charged to individuals to provide them with a copy of their PHI?

The HIPAA Privacy Rule permits a covered entity to charge a reasonable, cost-based fee for individuals (or their personal representatives) to receive (or direct to a third party) a copy of the individuals' PHI. In addition to being reasonable, the fee may include only certain labor, supply, and postage costs that may apply in providing the individual with the copy in the form and format and manner requested or agreed to by the individual. A covered entity may calculate this fee in three ways.

- Actual costs. A covered entity may calculate actual labor costs to fulfill the request, as long as the labor included is only for copying (and/or creating a summary or explanation if the individual chooses to receive a summary or explanation) and the labor rates used are reasonable for such activity. The covered entity may add to the actual labor costs any applicable supply (e.g., paper, or CD or USB drive) or postage costs. Covered entities that charge individuals actual costs based on each individual access request still must be prepared to inform individuals in advance of the approximate fee that may be charged for providing the individual with a copy of her PHI. An example of an actual labor cost calculation would be to time how long it takes for the workforce member of the covered entity (or business associate) to make and send the copy in the form and format and manner requested or agreed to by the individual and multiply the time by the reasonable hourly rate of the person copying and sending the PHI. What is reasonable for purposes of an hourly rate will vary depending on the level of skill needed to create and transmit the copy in the manner requested or agreed to by the individual (e.g., administrative level labor to make and mail a paper copy versus more technical skill needed to convert and transmit the PHI in a particular electronic format).
- Average costs. In lieu of calculating labor costs individually for each request, a covered entity can develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, as long as the types of labor costs included are the ones which the Privacy Rule permits to be included in a fee (e.g., labor costs for copying but not for search and retrieval) and are reasonable. Covered entities may add to that amount any applicable supply (e.g., paper, or CD or USB drive) or postage costs.
 - This standard rate can be calculated and charged as a per page fee only in cases where the PHI requested is maintained in paper form and the individual requests a paper copy of the PHI or asks that the paper PHI be scanned into an electronic format. Per page fees are not permitted for paper or electronic copies of PHI maintained electronically. OCR is aware that per page fees in many cases have become a proxy for fees charged for all types of access requests – whether electronic or paper – and that many states with authorized fee structures have not updated their laws to account for efficiencies that exist when generating copies of information maintained electronically. This practice has resulted in fees being charged to individuals for copies of their PHI that do not appropriately reflect the permitted labor costs associated with generating copies from information maintained in electronic form. Therefore, OCR does not consider per page fees for copies of PHI maintained electronically to be reasonable for purposes of 45 CFR 164.524(c)(4).
- Flat fee for electronic copies of PHI maintained electronically. A covered entity may charge individuals a flat fee for all standard requests for electronic copies of PHI maintained electronically, provided the fee does not exceed \$6.50, inclusive of all labor, supplies, and any applicable postage.

Are costs authorized by State fee schedules permitted to be charged to individuals when providing them with a copy of their PHI under the HIPAA Privacy Rule?

No, except in cases where the State authorized costs are the same types of costs permitted under 45 CFR 164.524(c)(4) of the HIPAA Privacy Rule, and are reasonable. The bottom line is that the costs authorized by the State must be those that are permitted by the HIPAA

Privacy Rule and must be reasonable. The HIPAA Privacy Rule at 45 CFR 164.524(c)(4) permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual. Thus, labor (e.g., for search and retrieval) or other costs not permitted by the Privacy Rule may not be charged to individuals even if authorized by State law. Further, a covered entity's fee for providing an individual with a copy of her PHI must be reasonable in addition to cost-based, and there may be circumstances where a State authorized fee is not reasonable, even if the State authorized fee covers only permitted labor, supply, and postage costs. For example, a State-authorized fee may be higher than the covered entity's cost to provide the copy of PHI. In addition, many States with authorized fee structures have not updated their laws to account for efficiencies that exist when generating copies of information maintained electronically. Therefore, these State authorized fees for copies of PHI maintained electronically may not be reasonable for purposes of 45 CFR 164.524(c)(4).

A State law requires that a health care provider give individuals one free copy of their medical records but HIPAA permits the provider to charge a fee. Does HIPAA override the State law?

No, so the health care provider must comply with the State law and provide the one free copy. In contrast to State laws that authorize higher or different fees than are permitted under HIPAA, HIPAA does not override those State laws that provide individuals with greater rights of access to their health information than the HIPAA Privacy Rule does. See 45 CFR 160.202 and 160.203. This includes State laws that: (1) prohibit fees to be charged to provide individuals with copies of their PHI; or (2) allow only lesser fees than what the Privacy Rule would allow to be charged for copies.

When do the HIPAA Privacy Rule limitations on fees that can be charged for individuals to access copies of their PHI apply to disclosures of the individual's PHI to a third party?

The fee limits apply when an individual directs a covered entity to send the PHI to the third party. Under the HIPAA Privacy Rule, a covered entity is prohibited from charging an individual who has requested a copy of her PHI more than a reasonable, cost-based fee for the copy that covers only certain labor, supply, and postage costs that may apply in fulfilling the request. See 45 CFR 164.524(c)(4). This limitation applies regardless of whether the individual has requested that the copy of PHI be sent to herself, or has directed that the covered entity send the copy directly to a third party designated by the individual (and it doesn't matter who the third party is). To direct a copy to a third party, the individual's access request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI. See 45 CFR 164.524(c)(3)(ii). Thus, written access requests by individuals to have a copy of their PHI sent to a third party that include these minimal elements are subject to the same fee limitations in the Privacy Rule that apply to requests by individuals to have a copy of their PHI sent to themselves. This is true regardless of whether the access request was submitted to the covered entity by the individual directly or forwarded to the covered entity by a third party on behalf and at the direction of the individual (such as by an app being used by the individual). Further, these same limitations apply when the individual's personal representative, rather than the individual herself, has made the request to send a copy of the individual's PHI to a third party.

In contrast, third parties often will directly request PHI from a covered entity and submit a written HIPAA authorization from the individual (or rely on another permission in the Privacy Rule) for that disclosure. Where the third party is initiating a request for PHI on its own

behalf, with the individual's HIPAA authorization (or pursuant to another permissible disclosure provision in the Privacy Rule), the access fee limitations do not apply. However, as described above, where the third party is forwarding - on behalf and at the direction of the individual - the individual's access request for a covered entity to direct a copy of the individual's PHI to the third party, the fee limitations apply.

We note that a covered entity (or a business associate) may not circumvent the access fee limitations by treating individual requests for access like other HIPAA disclosures – such as by having an individual fill out a HIPAA authorization when the individual requests access to her PHI (including to direct a copy of the PHI to a third party). As explained elsewhere in the guidance, a HIPAA authorization is not required for individuals to request access to their PHI, including to direct a copy to a third party – and because a HIPAA authorization requests more information than is necessary or that may not be relevant for individuals to exercise their access rights, requiring execution of a HIPAA authorization may create impermissible obstacles to the exercise of this right. Where it is unclear to a covered entity, based on the form of a request sent by a third party, whether the request is an access request initiated by the individual or merely a HIPAA authorization by the individual to disclose PHI to the third party, the entity may clarify with the individual whether the request was a direction from the individual or a request from the third party. OCR is open to engaging with the community on ways that technology could easily convey this information.

Finally, we note that disclosures to a third party made outside of the right of access under other provisions of the Privacy Rule still may be subject to the prohibition against sales of PHI (i.e., the prohibition against receiving remuneration for a disclosure of PHI at 45 CFR 164.502(a)(5)(ii)). Where the prohibition applies, a covered entity may charge only a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by other law or must have received a HIPAA authorization from the individual that states that the disclosure will involve remuneration to the covered entity.

May a health care provider withhold a copy of an individual's PHI from the individual who requested it because the covered entity used the individual's payment of the allowable fee for the copy to instead pay an outstanding bill for health care services provided to the individual?

No. Just as a covered entity may not withhold or deny an individual access to his PHI on the grounds that the individual has not paid the bill for health care services the covered entity provided to the individual, a covered entity may not withhold or deny access on the grounds that the covered entity used the individual's payment of the fee for a copy of his PHI to offset or pay the individual's outstanding bill for health care services.

Can an individual be charged a fee if the individual requests only to inspect her PHI at the covered entity (i.e., does not request that the covered entity produce a copy of the PHI)?

No. The fees that can be charged to individuals exercising their right of access to their PHI apply only in cases where the individual is to receive a copy of the PHI, versus merely being provided the opportunity to view and inspect the PHI. The HIPAA Privacy Rule provides individuals with the right to inspect their PHI held in a designated record set, either in addition to obtaining copies or in lieu thereof, and requires covered entities to arrange with the individual for a convenient time and place to inspect the PHI. See 45 CFR 164.524(c)(1) and (c)(2). Consequently, covered entities should have in place reasonable procedures to enable individuals to inspect their PHI, and requests for inspection should trigger minimal additional effort by the entity, particularly where the PHI requested is of the type easily

accessed onsite by the entity itself in the ordinary course of business. For example, covered entities could use the capabilities of Certified EHR Technology (CEHRT) to enable individuals to inspect their PHI, if the individuals agree to the use of this functionality.

Further, a covered entity may not charge an individual who, while inspecting her PHI, takes notes, uses a smart phone or other device to take pictures of the PHI, or uses other personal resources to capture the information. If the individual is making the copies of PHI using her own resources, the covered entity may not charge a fee for those copies, as the copying is being done by the individual and not the entity. A covered entity may establish reasonable policies and safeguards regarding an individual's use of her own camera or other device for copying PHI to assure that equipment or technology used by the individual is not disruptive to the entity's operations and is used in a way that enables the individual to copy or otherwise memorialize only the records to which she is entitled. Further, a covered entity is not required to allow the individual to connect a personal device to the covered entity's systems.

Right to Have PHI Sent Directly to a Designated Third Party

Can an individual, through the HIPAA right of access, have his or her health care provider or health plan send the individual's PHI to a third party?

Yes. If requested by an individual, a covered entity must transmit an individual's PHI directly to another person or entity designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI. See 45 CFR 164.524(c)(3)(ii). A covered entity may accept an electronic copy of a signed request (e.g., PDF or scanned image), an electronically executed request (e.g., via a secure web portal) that includes an electronic signature, or a faxed or mailed copy of a signed request.

The same requirements for providing the PHI to the individual, such as the timeliness requirements, fee limitations, prohibition on imposing unreasonable measures, and form and format requirements, apply when an individual directs that the PHI be sent to another person or entity. For example, just as when the individual requests a copy for herself, a covered entity cannot require that an individual make a separate in person trip to the covered entity's physical location for the purpose of making the request to transmit the individual's PHI to a person or entity designated by the individual. In addition, the individual can designate the form and format of the PHI and how the PHI is to be sent to the third party, and the covered entity must provide access in the requested form and format and manner if the PHI is "readily producible" in such a way. Whether PHI is "readily producible" depends on the capabilities of the covered entity and whether transmission or transfer of the PHI in the requested manner would present an unacceptable level of security risk to the PHI on the covered entity's systems (based on the covered entity's Security Rule risk analysis).

The following are just a few examples of how these provisions apply:

- A patient requests in writing that the hospital where she recently underwent a surgical procedure use its Certified EHR Technology (CEHRT) to send her discharge summary to her primary care physician, or to her own personal health record, and she supplies the corresponding Direct address (an electronic address for securely exchanging health information using the Direct technical standard).
- A patient sends a written request to his long-time physician asking the physician to download a copy of the PHI from his electronic medical record, and e-mail it in

- encrypted form to XYZ Research Institution, at XYZResearch@anywhere.com, so XYZ Research Institution can use his health information for research purposes.
- A patient requests in writing that her ob-gyn digitally transmit records of her latest pre-natal visit to a new pregnancy self-care app that she has on her mobile phone. The ob-gyn's EHR has the ready capability to establish the connection in a manner that does not present an unacceptable level of security risk to the PHI in the EHR or other of the ob-gyn's systems, based on the ob-gyn's Security Rule risk analysis.

In each of these three examples, the covered entity has the capability to transfer the PHI in the requested manner and doing so would not present an unacceptable level of security risk to the PHI in the covered entity's systems. Thus, after receiving the patient's written request, the covered entity has 30 days (or 60 days if an extension is applicable) to send the PHI to the designated recipient as directed by the individual. However, in most cases, it is expected that the use of technology will enable the covered entity to fulfill the individual's request in far fewer than 30 days.

Are there any limits or exceptions to the individual's right to have the individual's PHI sent directly to a third party?

The right of an individual to have PHI sent directly to a third party is an extension of the individual's right of access; consequently, all of the provisions that apply when an individual obtains access to her PHI apply when she directs a covered entity to send the PHI to a third party. As a result:

- This right applies to PHI in a designated record set;
- Covered entities must take action within 30 days of the request;
- Covered entities must provide the PHI in the form and format and manner of access requested by the individual if it is "readily producible" in that manner; and
- The individual may be charged only a reasonable, cost-based fee that complies with 45 CFR 164.524(c)(4).

Further, the same limited grounds for denial of access that apply when the individual is receiving the PHI directly apply in cases where the individual requests that the PHI be provided to a designated third party. See 45 CFR 164.524(a)(2) and (a)(3). Thus, for example, a covered entity may deny an individual's request to send PHI to a designated third party when the request is for psychotherapy notes or PHI for which a licensed health care professional has determined, exercising professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. The provisions of the Privacy Rule providing for review of certain denials of access apply in this circumstance as well. See 45 CFR 164.524(a)(3) and (a)(4). However, a covered entity may not deny an individual's access request to send PHI to a third party for other purposes. Thus, disagreement with the individual about the worthiness of the third party as a recipient of PHI, or even concerns about what the third party might do with the PHI (except for the express reasons listed in the Privacy Rule, such as in cases where life or physical safety is threatened), are not acceptable reasons to deny an individual's request.

Can an individual's personal representative, through the HIPAA right of access, have the individual's health care provider or health plan send the individual's PHI to a third party?

Yes. An individual's personal representative (generally, a person with authority under State law to make health care decisions for the individual) has the right both to receive a copy of PHI about the individual in a designated record set, and to direct the covered entity to

transmit a copy of the PHI to another person or entity, upon request, consistent with the scope of such representation and the requirements of 45 CFR 164.524. See 45 CFR 164.502(g). The same requirements for fulfilling an individual's request to send the individual's PHI to a third party (e.g., with respect to timeliness, form and format, bases for denial, fee limitations, etc.) also apply to requests made by an individual's personal representative.

What is the liability of a covered entity in responding to an individual's access request to send the individual's PHI to a third party?

Covered entities may rely on the information provided in writing by the individual about the identity of the designated person and where to send the PHI for purposes of verification of the designated third party as an authorized recipient. However, covered entities must implement reasonable safeguards in otherwise carrying out the request, such as taking reasonable steps to verify the identity of the individual making the access request and to enter the correct information into the covered entity's system. For example, while a covered entity is not required to confirm that the individual provided the correct e-mail address of the third party, the covered entity is required to have reasonable procedures to ensure that it correctly enters the provided e-mail address into the covered entity's system.

In addition, except in the limited circumstance described below, covered entities must safeguard the information in transit, and are responsible for breach notification and may be liable for impermissible disclosures of PHI that occur in transit. The only exception arises when an individual has requested that the PHI be sent to the third party by unencrypted e-mail or in another unsecure manner, which the individual has a right to request. As long as the individual was warned of and accepted the security risks to the PHI associated with the unsecure transmission, the covered entity is not responsible for breach notification or liable for disclosures that occur in transit.

Further, the covered entity is not liable for what happens to the PHI once the designated third party receives the information as directed by the individual in the access request.

What is a covered entity's obligation under the Breach Notification Rule if it transmits an individual's PHI to a third party designated by the individual in an access request, and the entity discovers the information was breached in transit?

If a covered entity discovers that the PHI was breached in transit to the designated third party, and the PHI was "unsecured PHI" as defined at 45 CFR 164.402, the covered entity generally is obligated to notify the individual and HHS of the breach and otherwise comply with the HIPAA Breach Notification Rule at 45 CFR 164, Subpart D. However, if the individual requested that the covered entity transmit the PHI in an unsecure manner (e.g., unencrypted), and, after being warned of the security risks to the PHI associated with the unsecure transmission, maintained her preference to have the PHI sent in that manner, the covered entity is not responsible for a disclosure of PHI while in transmission to the designated third party, including any breach notification obligations that would otherwise be required. Further, a covered entity is not liable for what happens to the PHI once the designated third party receives the information as directed by the individual in the access request.

Where the PHI that was breached is "secured" as provided for in the HHS Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>), the covered entity does not have reporting obligations under the Breach Notification Rule.

Why depend on the individual’s right of access to facilitate the disclosure of PHI to a third party – why not just have the individual execute a HIPAA authorization to enable the covered entity to make this disclosure?

The PHI that an individual wants to have disclosed to a third party under the HIPAA right of access also could be disclosed by a covered entity pursuant to a valid HIPAA authorization. However, there are differences between the two methods – the primary difference being that one is a required disclosure and one is a permitted disclosure -- that may make the right of access a more favorable choice for most disclosures the individual is initiating on her own behalf. These differences are illustrated in the following table:

HIPAA Authorization	Right of Access
Permits, but does not require, a covered entity to disclose PHI	Requires a covered entity to disclose PHI, except where an exception applies
Requires a number of elements and statements, which include a description of who is authorized to make the disclosure and receive the PHI, a specific and meaningful description of the PHI, a description of the purpose of the disclosure, an expiration date or event, signature of the individual authorizing the use or disclosure of her own PHI and the date, information concerning the individual’s right to revoke the authorization, and information about the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.	Must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI
No timeliness requirement for disclosing the PHI Reasonable safeguards apply (e.g., PHI must be sent securely)	Covered entity must act on request no later than 30 days after the request is received
Reasonable safeguards apply (e.g., PHI must be sent securely)	Reasonable safeguards apply, including a requirement to send securely; however, individual can request transmission by unsecure medium
No limitations on fees that may be charged to the person requesting the PHI; however, if the disclosure constitutes a sale of PHI, the authorization must disclose the fact of remuneration	Fees limited as provided in 45 CFR 164.524(c)(4)

In addition, the Privacy Rule permits covered entities to disclose PHI for treatment, payment and health care operations without the need to first obtain an individual’s authorization or receive an access request by the individual to have the individual’s PHI directed to a third party for such purposes. See 45 CFR 164.506. As a result, if an individual is seeking to have her PHI shared among her treating providers, the covered entities can and should do so; the individual should not have to facilitate this transmission by submitting an access request (and potentially having to wait up to 30 days for the information to be sent and be charged a fee) or by executing a HIPAA authorization. See the Fact Sheets on Understanding Some of

HIPAA's Permitted Uses and Disclosures at <http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/permitted-uses/index.html>.

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
<p>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)</p>	<p>Covered entity required by law to provide individuals with access upon request</p>
<p>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**)</p> <p>*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</p> <p>**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</p>	<p>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)</p>
<p>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</p>	<p>Prompt access is encouraged but covered entities may take no longer than 30 days from receipt to act on a request for access (and</p>

EHR Incentive Program	HIPAA Privacy Rule
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)	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.

Other Access Topics

Under HIPAA, when can a family member of an individual access the individual’s PHI from a health care provider or health plan?

The HIPAA Privacy Rule provides individuals with the right to access their medical and other health records from their health care providers and health plans, upon request. The Privacy Rule generally also gives the right to access the individual’s health records to a personal representative of the individual. Under the Rule, an individual’s personal representative is someone authorized under State or other applicable law to act on behalf of the individual in making health care related decisions. With respect to deceased individuals, the individual’s personal representative is an executor, administrator, or other person who has authority under State or other law to act on behalf of the deceased individual or the individual’s estate. Thus, whether a family member or other person is a personal representative of the individual, and therefore has a right to access the individual’s PHI under the Privacy Rule, generally depends on whether that person has authority under State law to act on behalf of the individual. See 45 CFR 164.502(g) and 45 CFR 164.524.

In cases where a family member may not have the requisite authority to be a personal representative, an individual still has the ability, under the HIPAA right of access, to direct a covered entity to transmit a copy of the individual’s PHI to the family member, and the

covered entity must comply with the request, except in limited circumstances. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI. See 45 CFR 164.524(c)(3)(ii).

Outside of the HIPAA right of access, other provisions in the Privacy Rule address disclosures to family members. Specifically, a covered entity is permitted to share information with a family member or other person involved in an individual's care or payment for care as long as the individual does not object. In cases where the individual is incapacitated, a covered entity may share the individual's information with the family member or other person if the covered entity determines, based on professional judgment, that the disclosure is in the best interest of the individual. If the individual is deceased, a covered entity may make the disclosure unless doing so is inconsistent with any prior expressed preference of the individual. These disclosures are generally limited to the health information that is relevant to the person's involvement in the individual's care or payment for care. See 45 CFR 164.510(b).

Finally, a covered entity also is permitted to disclose the health information about an individual to any person, including a family member, if the individual provides a prior written authorization for the disclosure. See 45 CFR 164.508.

May a covered entity accept standing requests from individuals to access their PHI or to have their PHI sent to a third party of their choice?

Yes, and covered entities should have processes in place that enable individuals to receive access to their PHI, including to direct a copy of their PHI to a third party of their choice, on a standing, regular basis, without requiring individuals to repeat their requests for access every time a copy of their PHI is to be sent or otherwise made accessible. Further, covered entities should take advantage of technology and tools that automate such regular access.