10. Section 164.524—Access of Individuals to Protected Health Information

Proposed Rule

Section 164.524 of the Privacy Rule currently establishes, with limited exceptions, an enforceable means by which individuals have a right to review or obtain copies of their protected health information to the extent such information is maintained in the designated record set(s) of a covered entity. An individual's right of access exists regardless of the format of the protected health information, and the standards and implementation specifications that address individuals' requests for access and timely action by the covered entity (i.e., provision of access, denial of access, and documentation) apply to an electronic environment in a similar manner as they do to a paper-based environment. See The HIPAA Privacy Rule's Right of Access and Health Information Technology (providing guidance with respect to how § 164.524 applies in an electronic environment and how health information technology can facilitate providing individuals with this important privacy right), available at: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf.*

Section 13405(e) of the HITECH Act strengthens the Privacy Rule's right of access with respect to covered entities that use or maintain an electronic health record (EHR) on an individual. Section 13405(e) provides that when a covered entity uses or maintains an EHR with respect to protected health information of an individual, the individual shall have a right to obtain from the covered entity a copy of such information in an electronic format and the individual may direct the covered entity to transmit such copy directly to the individual's designee, provided that any such choice is clear, conspicuous, and specific. Section 13405(e) also provides that any fee imposed by the covered entity for providing such an electronic copy shall not be greater than the entity's labor costs in responding to the request for the copy.

Section 13405(e) applies by its terms only to protected health information in EHRs. However, incorporating these new provisions in such a limited manner in the Privacy Rule could result in a complex set of disparate requirements for access to protected health information in EHR systems versus other types of electronic records systems. As such, the Department proposed to use its authority under section 264(c) of HIPAA to prescribe the rights individuals should have with respect to their individually identifiable health information to strengthen the right of access as provided under section 13405(e) of the HITECH Act more uniformly to all protected health information maintained in one or more designated record sets electronically, regardless of whether the designated record set is an EHR. The public comments and final regulation on the scope are discussed here. The proposed amendments to each provision implicated by section 13405(e), together with the public comments and final regulation, are discussed more specifically in separate sections below.

Overview of Public Comments

Most commenters were opposed to the proposal to expand the scope of the individual access provision to include all electronic designated record sets and favored limiting the requirement to EHRs. These commenters felt that limiting the access provision to EHRs was consistent with congressional intent and questioned the authority of the Department to expand the scope. Commenters also argued that having disparate requirements for different systems would not be confusing, and requiring electronic access to electronic designated record sets that are not EHRs would be highly burdensome for covered entities. Specifically, commenters stated that the proposed requirement for electronic access would include numerous types of legacy systems, many of which are incapable of producing reports in easily readable formats that can be transmitted electronically. These commenters indicated that a significant amount of information technology development and investment would be needed to comply with this requirement if it applies to all electronic designated record sets.

A number of consumer advocates supported the expanded scope to include all electronic designated records sets in addition to EHRs. These commenters felt that this would provide complete transparency for consumers, help individuals gain access to their medical records and make better-informed decisions about their health care, and promote consistent and uniform practices.

Final Rule

The final rule adopts the proposal to amend the Privacy Rule at § 164.524(c)(2)(ii) to require that if an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. In such cases, to the extent possible, we expect covered entities to provide the individual with a machine readable copy of the individual's protected health information. The Department considers machine readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the individual with an electronic copy of the protected health information in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats.

We disagree with commenters that questioned the Department's authority to extend the strengthened electronic access right to all protected health information maintained electronically in designated record sets, and believe that this extended electronic right of access is important for individuals as covered entities increasingly transition from paper to electronic records. With regard to the additional burdens on covered entities, we note that providing access to protected health information held in electronic designated record sets was already required under the Privacy Rule at § 164.524, which applies to protected health information in both paper and electronic designated record sets, and which requires providing the copy in the form and format requested by the individual, including electronically, if it is readily producible in such form and format. We anticipate the additional burden to be small due to the flexibility permitted in satisfying this new requirement, as discussed in the section on Form and Format.

Response to Other Public Comments

Comment: Some commenters worried that giving individuals access to administrative systems (in contrast to clinical systems) would present a security concern to covered entities.

Response: Covered entities are not required by this provision to provide individuals with direct access to their systems. They must only provide individuals with an electronic copy of their protected health information.

Comment: Commenters requested clarification on what constitutes an EHR.

Response: Under this final rule, the requirement to provide individuals with access to an electronic copy includes all

protected health information maintained in an electronic designated record set held by a covered entity. Because we are not limiting the right of electronic access to EHRs, we do not believe there is a need to define or further clarify the term at this time.

Comment: One commenter requested clarification that this electronic access requirement preempts State laws that diminish, block, or limit individual access to their records.

Response: We clarify that this HIPAA electronic right of access requirement does preempt contrary State law unless such law is more stringent. In the case of right of access, more stringent means that such State law permits greater rights of access to the individual.

Comment: Several commenters sought clarification of how the new e-access provisions would apply to business associates. One commenter asked whether business associates could continue to provide patients access to records when permitted and acting on behalf of a covered entity. Another commenter asked whether business associates are required to provide information to covered entities and not to individuals directly. One commenter was opposed to direct access from a business associate because of security concerns and increased burden on business associates if corrections are needed.

Response: How and to what extent a business associate is to support or fulfill a covered entity's obligation to provide individuals with electronic access to their records will be governed by the business associate agreement between the covered entity and the business associate. For example, the business associate agreement may provide for the business associate to give copies of the requested information directly to the individual, or to the covered entity for the covered entity to provide the copies to the individual. There is no separate requirement on business associates to provide individuals with direct access to their health records, if that is not what has been agreed to between the covered entity and the business associate in the business associate agreement.

a. Form and Format

Proposed Rule

Section 164.524(c)(2) of the Privacy Rule currently requires a covered entity to provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format, or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual. Section 13405(e) of the HITECH Act expands this requirement by explicitly requiring a covered entity that uses or maintains an EHR with respect to protected health information to provide the individual with a copy of such information in an electronic format.

We proposed to implement this statutory provision, in conjunction with our broader authority under section 264(c) of HIPAA, by requiring, in proposed § 164.524(c)(2)(ii), that if the protected health information requested is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. This provision would require any covered entity that electronically maintains the protected health information about an individual, in one or more designated record sets, to provide the individual with an electronic copy of such information (or summary or explanation if agreed to by the individual in accordance with proposed § 164.524(c)(2)(iii)) in the electronic form and format requested or in an otherwise agreed upon electronic form and format. While an individual's right of access to an electronic copy of protected health information is currently limited under the Privacy Rule by whether the form or format requested is readily producible, covered entities that maintain such information electronically in a designated record set would be required under these proposed modifications to provide some type of electronic copy, if requested by an individual.

Because we did not want to bind covered entities to standards that may not yet be technologically mature, we proposed to permit covered entities to make some other agreement with individuals as to an alternative means by which they may provide a readable electronic copy to the extent the requested means is not readily producible. If, for example, a covered entity received a request to provide electronic access via a secure web-based portal, but the only readily producible version of the protected health information was in portable document format (PDF), proposed § 164.524(c)(2)(ii) would require the covered entity to provide the individual with a PDF copy of the protected health information, if agreed to by the covered entity and the individual. We noted that while a covered entity may provide individuals with limited access rights to their EHR, such as through a secure web-based portal, nothing under the current Rule or proposed modifications would require a covered entity to have this capability.

We noted that the option of arriving at an alternative agreement that satisfies both parties is already part of the requirement to provide access under § 164.524(c)(2)(i), so extension of such a requirement to electronic access should present few implementation difficulties. Further, as with other disclosures of protected health information, in providing the individual with an electronic copy of protected health information through a web-based portal, email, on portable electronic media, or other means, covered entities should ensure that reasonable safeguards are in place to protect the information. We also noted that the proposed modification presumes that covered entities have the capability of providing an electronic copy of protected health information maintained in their designated record set(s) electronically through a secure web-based portal, via email, on portable electronic media, or other manner. We invited public comment on this presumption.

Overview of Public Comments

We received many comments and requests for clarification and guidance regarding the permitted methods for offering protected health information on electronic media, and the acceptable form and format of the electronic copy. Several commenters suggested that covered entities be permitted flexibility in determining available electronic formats and requested clarification on what is considered "readily producible." These commenters expressed concerns that a limited number of permissible electronic formats may result in a situation where protected health information could not be converted from a particular electronic system. Other commenters indicated that there should be minimum standards and clearly defined media that are permissible to meet this requirement. One commenter felt that this requirement is important but should be deferred until covered entities have improved their technological capabilities.

Many commenters requested guidance on how to proceed if a covered entity and an individual are unable to come to an agreement on the medium of choice and what is expected in terms of accommodating the individual's medium of choice. Some commenters suggested various alternate solutions if

an agreement cannot be reached, including any readily producible format, PDF, or hard copy protected health information. Some covered entities felt that individuals should not have an unlimited choice in terms of the electronic media they are willing to accept, and should only be permitted to confine their choices of electronic media to a couple of options that the covered entity has available.

Final Rule

The final rule adopts the proposal to require covered entities to provide electronic information to an individual in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. We recognize that what is available in a readable electronic form and format will vary by system and that covered entities will continue to improve their technological capabilities over time. We therefore allow covered entities the flexibility to provide readily producible electronic copies of protected health information that are currently available on their various systems. A covered entity is not required to purchase new software or systems in order to accommodate an electronic copy request for a specific form that is not readily producible by the covered entity at the time of the request, provided that the covered entity is able to provide some form of electronic copy. We note that some legacy or other systems may not be capable of providing any form of electronic copy at present and anticipate that some covered entities may need to make some investment in order to meet the basic requirement to provide some form of electronic copy.

We agree with covered entities that individuals should not have an unlimited choice in the form of electronic copy requested. However, covered entities must still provide individuals with some kind of readable electronic copy. 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 their systems. If the individual declines to accept any of the electronic formats that are readily producible by the covered entity, the covered entity must provide a hard copy as an option to fulfill the access request. While we remain neutral on the type of technology that covered entities may adopt, a PDF is a widely recognized format that would satisfy the electronic access requirement if it is the individual's requested format or if the individual agrees to accept a PDF instead of the individual's requested format. Alternatively, there may be circumstances where an individual prefers a simple text or rich text file and the covered entity is able to accommodate this preference. A hard copy of the individual's protected health information would not satisfy the electronic access requirement. However, a hard copy may be provided if the individual decides not to accept any of the electronic formats offered by the covered entity.

Response to Other Public Comments

Comment: Several covered entities commented on the form of a request for access to electronic protected health information. Some expressed appreciation for permitting an electronic request process, including e-signatures and authentication. Some expressed opposition to the requirement for a signed request in writing, as it would be highly burdensome and cause delays. Covered entities sought guidance on elements that would be required or permitted in a request form for individuals.

Response: We clarify that the requirement at § 164.524(b)(1), which states that the covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement, remains unchanged. Therefore, covered entities may at their option require individuals to make requests for electronic copies of their protected health information in writing. We note that the Privacy Rule allows for electronic documents to qualify as written documents, as well as electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law. If the covered entity chooses to require a written request, it has flexibility in determining what information to put into the request form. However, the request form may not be in any way designed to discourage an individual from exercising his or her right. A covered entity may also choose to accept an individual's oral request for an electronic copy of their protected health information without written signature or documentation.

Comment: We received several comments on the content that covered entities are required to provide in response to an electronic access request. Some commenters felt that there should be a defined minimum set of data elements to satisfy this requirement, particularly for non-EHR data. Covered entities also requested clarification on how to handle links to images or other data.

Response: We clarify that just as is currently required for hard copy protected health information access requests, covered entities must provide an electronic copy of all protected health information about the individual in an electronically maintained designated record set, except as otherwise provided at § 164.524(a). If the designated record set includes electronic links to images or other data, the images or other data that is linked to the designated record set must also be included in the electronic copy provided to the individual. The electronic copy must contain all protected health information electronically maintained in the designated record set at the time the request is fulfilled. The individual may request, however, only a portion of the protected health information electronically maintained in the designated record set, in which case the covered entity is only required to provide the requested information.

Comment: One commenter asserted that the request for protected health information should only apply to protected health information the covered entity has at the time of the request, not any additional protected health information that it obtains while processing the request.

Response: We clarify that the electronic copy must reflect all electronic protected health information held by the covered entity in a designated record set, or the subset of electronic protected health information specifically requested by the individual, at the time the request is fulfilled.

Comment: One commenter asked for confirmation that the new electronic requirement does not include a requirement to scan paper and provide electronic copies of records held in paper form.

Response: We clarify that covered entities are not required to scan paper documents to provide electronic copies of records maintained in hard copy. We note that for covered entities that have mixed media, it may in some cases be easier to scan and provide all records in electronic form rather than provide a combination of electronic and hard copies, however this is in no way required.

Comment: Many commenters expressed security concerns related to this new requirement. Covered entities felt that they should not have to use portable devices brought by individuals (particularly flash drives), due to the security risks that this would introduce to their systems. Some covered entities

additionally asserted that requiring the use of individually-supplied media is prohibited by the Security Rule, based on the risk analysis determination of an unacceptable risk to the confidentiality, integrity and availability of the covered entity's electronic protected health information.

Response: We acknowledge these security concerns and agree with commenters that it may not be appropriate for covered entities to accept the use of external portable media on their systems. 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. 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 protected health information, such as through email.

Comment: Several commenters specifically commented on the option to provide electronic protected health information via unencrypted email. Covered entities requested clarification that they are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. Some felt that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on covered entities. Covered entities also requested clarification that they would not be responsible for breach notification in the event that unauthorized access of protected health information occurred as a result of sending an unencrypted email based on an individual's request. Finally, one commenter emphasized the importance that individuals are allowed to decide if they want to receive unencrypted emails.

Response: We clarify that covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. We disagree that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on covered entities and believe this is a necessary step in protecting the protected health information. We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual.

b. Third Parties

Proposed Rule

Section 164.524(c)(3) of the Privacy Rule currently requires the covered entity to provide the access requested by the individual in a timely manner, which includes arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of protected health information at the individual's request. The Department had previously interpreted this provision as requiring a covered entity to mail the copy of protected health information to an alternative address requested by the individual, provided the request was clearly made by the individual and not a third party. Section 13405(e)(1) of the HITECH Act provides that if the individual chooses, he or she has a right to direct the covered entity to transmit an electronic copy of protected health information in an EHR directly to an entity or person designated by the individual, provided that such choice is clear, conspicuous, and specific.

Based on section 13405(e)(1) of the HITECH Act and our authority under section 264(c) of HIPAA, we proposed to expand § 164.524(c)(3) to expressly provide that, if requested by an individual, a covered entity must transmit the copy of protected health information directly to another person designated by the individual. This proposed amendment is consistent with the Department's prior interpretation on this issue and would apply without regard to whether the protected health information is in electronic or paper form. We proposed to implement the requirement of section 13405(e)(1) that the individual's "choice [be] clear, conspicuous, and specific" by requiring that the individual's request be "in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information." We noted that the Privacy Rule allows for electronic documents to qualify as written documents for purposes of meeting the Rule's requirements, as well as electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law. Thus, a covered entity could employ an electronic process for receiving an individual's request to transmit a copy of protected health information to his or her designee under this proposed provision. Whether the process is electronic or paper-based, a covered entity must implement reasonable policies and procedures under § 164.514(h) to verify the identity of any person who requests protected health information, as well as implement reasonable safeguards under § 164.530(c) to protect the information that is used or disclosed.

Overview of Public Comments

Commenters requested clarification regarding the proposal to transmit an electronic copy of protected health information to another person designated by the individual. In particular, covered entities sought clarification on whether or not an authorization is required prior to transmitting the requested electronic protected health information to a third party designated by the individual. Some commenters supported the ability to provide electronic protected health information access to third parties without individual authorization, while others felt that authorization should be required. Covered entities requested clarification that they are not liable when making reasonable efforts to verify the identity of a third party recipient identified by the individual.

Final Rule

The final rule adopts the proposed amendment § 164.524(c)(3) to expressly provide that, if requested by an individual, a covered entity must transmit the copy of protected health information directly to another person designated by the individual. In contrast to other requests under § 164.524, when an individual directs the covered entity to send the copy of protected health information to another designated person, the request must be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the protected health information. If a covered entity has decided to require all access requests in writing, the third party recipient information and signature by the individual can be included in the same written request; no additional or separate written request is

required. This written request for protected health information to be sent to a designated person is distinct from an authorization form, which contains many additional required statements and elements (see § 164.508(c)). Covered entities may rely on the information provided in writing by the individual when providing protected health information to a third party recipient identified by the individual, but must also implement reasonable policies and procedures under § 164.514(h) to verify the identity of any person who requests protected health information, as well as implement reasonable safeguards under § 164.530(c) to protect the information that is used or disclosed. For example, reasonable safeguards would not require the covered entity to confirm that the individual provided the correct email address of the third party, but would require reasonable procedures to ensure that the covered entity correctly enters the email address into its system.

c. Fees

Proposed Rule

Section 164.524(c)(4) of the Privacy Rule currently permits a covered entity to impose a reasonable, cost-based fee for a copy of protected health information (or a summary or explanation of such information). However, such a fee may only include the cost of: (1) The supplies for, and labor of, copying the protected health information; (2) the postage associated with mailing the protected health information, if applicable; and (3) the preparation of an explanation or summary of the protected health information, if agreed to by the individual. With respect to providing a copy (or summary or explanation) of protected health information from an EHR in electronic form, however, section 13405(e)(2) of the HITECH Act provides that a covered entity may not charge more than its labor costs in responding to the request for the copy.

In response to section 13405(e)(2) of the HITECH Act, we proposed to amend § 164.524(c)(4)(i) to identify separately the labor for copying protected health information, whether in paper or electronic form, as one factor that may be included in a reasonable cost-based fee. While we did not propose more detailed considerations for this factor within the regulatory text, we retained all prior interpretations of labor with respect to paper copies—that is, that the labor cost of copying may not include the costs associated with searching for and retrieving the requested information. With respect to electronic copies, we asserted that a reasonable cost-based fee includes costs attributable to the labor involved to review the access request and to produce the electronic copy, which we expected would be negligible. However, we did not consider a reasonable cost-based fee to include a standard "retrieval fee" that does not reflect the actual labor costs associated with the retrieval of the electronic information or that reflects charges that are unrelated to the individual's request (e.g., the additional labor resulting from technical problems or a workforce member's lack of adequate training). We invited public comment on this aspect of our rulemaking, specifically with respect to what types of activities related to managing electronic access requests should be compensable aspects of labor.

We also proposed to amend § 164.524(c)(4)(ii) to provide separately for the cost of supplies for creating the paper copy or electronic media (i.e., physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media. This reorganization and the addition of the phrase "electronic media" reflected our understanding that since section 13405(e)(2) of the HITECH Act permits only the inclusion of labor costs in the charge for electronic copies, it by implication excludes charging for the supplies that are used to create an electronic copy of the individual's protected health information, such as the hardware (computers, scanners, etc.) or software that is used to generate an electronic copy of an individual's protected health information in response to an access request. We noted that this limitation is in contrast to a covered entity's ability to charge for supplies for hard copies of protected health information (e.g., the cost of paper, the prorated cost of toner and wear and tear on the printer). See 65 FR 82462, 82735, Dec. 28, 2000 (responding to a comment seeking clarification on "capital cost for copying" and other supply costs by indicating that a covered entity was free to recoup all of their reasonable costs for copying). We asserted that this interpretation was consistent with the fact that, unlike a hard copy, which generally exists on paper, an electronic copy exists independent of media, and can be transmitted securely via multiple methods (e.g., email, a secure web-based portal, or an individual's own electronic media) without accruing any ancillary supply costs. We also noted, however, that our interpretation of the statute would permit a covered entity to charge a reasonable and cost-based fee for any electronic media it provided, as requested or agreed to by an individual.

While we proposed to renumber the remaining factors at § 164.524(c)(4), we did not propose to amend their substance. With respect to § 164.524(c)(4)(iii), however, we noted that our interpretation of the statute would permit a covered entity to charge for postage if an individual requests that the covered entity transmit portable media containing an electronic copy through mail or courier (e.g., if the individual requests that the covered entity save protected health information to a CD and then mail the CD to a designee).

Overview of Public Comments

Commenters generally supported and appreciated the inclusion of a reasonable, cost-based fee that includes both labor and, in some cases, supply costs to support the new electronic access requirement. Several commenters disagreed that the cost related to reviewing and responding to requests would be negligible, particularly if the scope includes information in designated record sets and not only EHRs, since more technically trained staff would be necessary to perform this function.

Commenters provided many suggestions of costs that should be permitted in the fees, including those associated with labor, materials, systems, retrieval (particularly for old data maintained in archives, backup media or legacy systems), copying, transmission, and capital to recoup the significant investments made for data access, storage and infrastructure. Commenters offered additional suggestions on labor-related costs, including: skilled technical staff time; time spent recovering, compiling, extracting, scanning and burning protected health information to media, and distributing the media; and preparation of an explanation or summary if appropriate. Suggestions of materials-related costs included: CDs, flash drives, tapes or other portable media; new types of technology needed to comply with individual requests; office supplies; and mail copies. Systems-related costs included: software necessary to conduct protected health information searches; and implementation and maintenance of security systems and secure connectivity.

Final Rule

The final rule adopts the proposed amendment at § 164.524(c)(4)(i) to identify separately the labor for copying protected health information, whether

in paper or electronic form, as one factor that may be included in a reasonable cost-based fee. We acknowledge commenters' assertions that the cost related to searching for and retrieving electronic protected health information in response to requests would be not be negligible, as opposed to what we had anticipated, particularly in regards to designated record set access that will require more technically trained staff to perform this function. We clarify that labor costs included in a reasonable cost-based fee could include skilled technical staff time spent to create and copy the electronic file, such as compiling, extracting, scanning and burning protected health information to media, and distributing the media. This could also include the time spent preparing an explanation or summary of the protected health information, if appropriate.

The final rule also adopts the proposed amendment at § 164.524(c)(4)(ii) to provide separately for the cost of supplies for creating the paper copy or electronic media (i.e., physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media. We do not require that covered entities obtain new types of technology needed to comply with specific individual requests, and therefore the cost of obtaining such new technologies is not a permissible fee to include in the supply costs.

With respect to § 164.524(c)(4)(iii), we clarify that a covered entity is permitted to charge for postage if an individual requests that the covered entity transmit portable media containing an electronic copy through mail or courier (e.g., if the individual requests that the covered entity save protected health information to a CD and then mail the CD to a designee).

Fees associated with maintaining systems and recouping capital for data access, storage and infrastructure are not considered reasonable, cost-based fees, and are not permissible to include under this provision. Covered entities are not required to adopt or purchase new systems under this provision, and thus any costs associated with maintaining them are present regardless of the new electronic access right. Additionally, although the proposed rule indicated that a covered entity could charge for the actual labor costs associated with the retrieval of electronic information, in this final rule we clarify that a covered entity may not charge a retrieval fee (whether it be a standard retrieval fee or one based on actual retrieval costs). This interpretation will ensure that the fee requirements for electronic access are consistent with the requirements for hard copies, which do not allow retrieval fees for locating the data.

Response to Other Public Comments

Comment: Commenters requested clarification on how to proceed when State laws designate fees.

Response: When a State law provides a limit on the fee that a covered entity may charge for a copy of protected health information, this is relevant in determining whether a covered entity's fee is "reasonable" under § 164.524(c)(4). A covered entity's fee must be both reasonable and cost-based. For example, if a State permits a charge of 25 cents per page, but a covered entity is able to provide an electronic copy at a cost of five cents per page, then the covered entity may not charge more than five cents per page (since that is the reasonable and cost-based amount). Similarly, if a covered entity's cost is 30 cents per page but the State law limits the covered entity's charge to 25 cents per page, then the covered entity may not charge more than 25 cents per page (since charging 30 cents per page would be the cost-based amount, but would not be reasonable in light of the State law).

Comment: One commenter suggested that labor-related costs should include preparation of an affidavit certifying that the information is a true and correct copy of the records.

Response: We do not consider the cost to prepare an affidavit to be a copying cost. Thus, where an individual requests that an affidavit accompany the copy of protected health information requested by the individual for litigation purposes or otherwise, a covered entity may charge the individual for the preparation of such affidavit and is not subject to the reasonable, cost-based fee limitations of § 164.524(c)(4). However, a covered entity may not withhold an individual's copy of his or her protected health information for failure by the individual to pay any fees for services above and beyond the copying, such as for preparing an affidavit.

Comment: Some commenters recommended defining the following terms: "preparing," "producing," and "transmitting."

Response: We decline to define the terms "preparing," "producing," and "transmitting," as we believe the terms have been adequately understood and utilized in the context of hard copy access to protected health information.

d. Timeliness

Proposed Rule

We requested comment on one aspect of the right to access and obtain a copy of protected health information which the HITECH Act did not amend. In particular, the HITECH Act did not change the timeliness requirements for provision of access at § 164.524(b). Under the current requirements, a request for access must be approved or denied, and if approved, access or a copy of the information provided, within 30 days of the request. In cases where the records requested are only accessible from an off-site location, the covered entity has an additional 30 days to respond to the request. In extenuating circumstances where access cannot be provided within these timeframes, the covered entity may have a one-time 30-day extension if the individual is notified of the need for the extension within the original timeframes.

With regard to the timeliness of the provision of access, we recognized that with the advance of EHRs, there is an increasing expectation and capacity to provide individuals with almost instantaneous electronic access to the protected health information in those records through personal health records or similar electronic means. On the other hand, we did not propose to limit the right to electronic access of protected health information to certified EHRs, and the variety of electronic systems that are subject to this proposed requirement would not all be able to comply with a timeliness standard based on personal health record capabilities. It was our assumption that a single timeliness standard that would address a variety of electronic systems, rather than having a multitude of standards based on system capacity, would be the preferred approach to avoid workability issues for covered entities. Even under a single standard, nothing would prevent users of EHR systems from exceeding the Privacy Rule's timeliness requirements for providing access to individuals. Additionally, the Medicare and Medicaid EHR Incentive Programs (the "meaningful use" programs) require users of Certified EHR Technology to provide individuals with expedited access to information. Based on the assumption that a single standard would be the preferred approach under the Privacy Rule, we requested public comment on an appropriate, common timeliness standard for the provision of access by covered entities with electronic designated record sets generally. We specifically requested comment on aspects of existing systems

that would create efficiencies in processing of requests for electronic information, as well as those aspects of electronic systems that would provide little change from the time required for processing a paper record. Alternatively, we requested comment on whether the current standard could be altered for all systems, paper and electronic, such that all requests for access should be responded to without unreasonable delay and not later than 30 days.

We also requested public comment on whether, contrary to our assumption, a variety of timeliness standards based on the type of electronic designated record set is the preferred approach and if so, how such an approach should be implemented.

Finally, we requested comment on the time necessary for covered entities to review access requests and make necessary determinations, such as whether the granting of access would endanger the individual or other persons so as to better understand how the time needed for these reviews relates to the overall time needed to provide the individual with access. Further, we requested comment generally on whether the provision which allows a covered entity an additional 30 days to provide access to the individual if the protected health information is maintained off-site should be eliminated altogether for both paper and electronic records, or at least for protected health information maintained or archived electronically because the physical location of electronic data storage is not relevant to its accessibility.

Overview of Public Comments

Commenters generally supported maintaining the same timeframe for response for both paper and electronic records and not modifying the existing timeframes for response. Commenters espoused many rationales for maintaining a single standard and the existing response standards, including that off-site electronic storage with back-up tapes will require time to obtain the electronic media, multiple electronic systems may need to be accessed, some systems may not have data stored in useable formats requiring time to convert data, and time may be required to obtain data from business associates and subcontractors.

Some commenters acknowledged that electronic records may be easier to access, but review of records and verification processes would still require time that cannot be shortcut because a record is electronic. One commenter acknowledged that shorter times may be achievable when specific data set standards are established and covered entities have electronic records in place. One commenter believed that electronic records could be furnished in a much shorter timeframe, such as two business days.

Several commenters suggested responses be done in much shorter timeframes, such as instantly, within one day or three days. One commenter noted that meaningful use standards required access within three days for 50 percent of patients. These commenters suggested alternative timeframes for adoption, such as allowing 60 days for response due to off-site storage issues and potential for multiple requests. One commenter suggested 30 and 60 day times were unworkable and another commenter suggested eliminating the 30 day extension for off-site record storage. One commenter suggested 30 days may be longer than is necessary, but cautioned against mandates that would unreasonably divert provider resources (e.g., five days would be unreasonable when a provider must take time to include explanatory notes).

Final Rule

The final rule modifies the timeliness requirements for right to access and to obtain a copy of protected health information at § 164.524(b). We remove the provision at § 164.524(b)(2)(ii) that permits 60 days for timely action when protected health information for access is not maintained or accessible to the covered entity on-site. We retain and renumber as necessary the provision at § 164.524(b)(2)(iii) that permits a covered entity a one-time extension of 30 days to respond to the individual's request (with written notice to the individual of the reasons for delay and the expected date by which the entity will complete action on the request).

We believe the 30 day timeframe for access is appropriate and achievable by covered entities given the increasing expectation and capacity to provide individuals with almost instantaneous electronic access to the protected health information in those records through personal health records or similar electronic means. While a covered entity is permitted 30 days to provide access (with a 30-day extension when necessary), we encourage covered entities to provide individuals with access to their information sooner, and to take advantage of technologies that provide individuals with immediate access to their health information. Nevertheless, for covered entities that continue to make use of off-site storage or have additional time constraints to providing access, the 30 day extension remains available for a covered entity to exercise. This means, for example, that a covered entity must provide an individual with access to off-site records within 30 days of the individual's request when possible, with a 30-day extension available (for a total of 60 days, in contrast to the current law that permits up to 90 days to provide the individual with access to such records).

We decline to establish separate timeframes for timely access based upon whether the protected health information to be accessed is paper or electronic. Commenters generally supported adoption of a single standard rather than differing standards based upon whether a record is paper or electronic and no comments provided compelling reasons to establish differing standards.

Response to Other Public Comments

Comment: One commenter asked for clarification as to when the time period for responding to a response begins if the parties spend significant time attempting to reach agreement on the format of the electronic copy.

Response: We confirm that the time period for responding to a request for access begins on the date of the request. Covered entities that spend significant time before reaching agreement on the electronic format for a response are using part of the 30 days permitted for response.

Comment: One commenter suggested there should be a transition period for those covered entities that do not currently have the capability to meet the electronic access requirement.

Response: We decline to implement a transition period for access to electronic copies of protected health information. Covered entities are already subject to the hard copy access requirement for all information held in designated record sets, including electronic designated record sets, and the new requirement for electronic copies gives covered entities the flexibility to provide an electronic copy in a form that is readily producible. We do not believe additional time is needed to provide electronic copies of protected health information that are readily producible.

11. Other Technical Changes and Conforming Changes

Proposed Rule

We proposed to make a number of technical and conforming changes to the Privacy Rule to fix minor problems, such as incorrect cross-references, mistakes of grammar, and typographical errors. These changes are shown in Table 3 below.

TABLE 3—TECHNICAL AND CONFORMING CHANGES

Regulation section	Current language	Proposed change	Reason for change
164.510(b)(2)(iii)	"based the exercise of professional Judgment".	Insert "on" after "based"	Correct typographical error.
164.512(b)(1)	"Permitted disclosures" and "may disclose".	Insert "uses and" and "use or" before "disclosures" and "disclose," respectively.	Correct inadvertent omission.
164.512(e)(1)(iii)	"seeking protecting health information".	Change "protecting" to "protected"	Correct typographical error.
164.512(e)(1)(vi)	"paragraph (e)(1)(iv) of this section"	Change "(e)(1)(iv)" to "(e)(1)(v)"	Correct cross-reference.
164.512(k)(3)	"authorized by 18 U.S.C. 3056, or to foreign heads of state, or to for the conduct of investigations".	Remove the comma after "U.S.C. 3056" and the "to" before "for".	Correct typographical errors.

In addition to the above technical changes, we proposed to make a few clarifications to existing text in various provisions of the regulation not otherwise addressed in the above preamble. These are as follows.

1. Section 164.506(c)(5) permits a covered entity to disclose protected health information "to another covered entity that participates in the organized health care arrangement." We proposed to change the words "another covered entity that participates" to "other participants" because not all participants in an organized health care arrangement may be covered entities; for example, some physicians with staff privileges at a hospital may not be covered entities.

2. Section 164.510(a)(1)(ii) permits the disclosure of directory information to members of the clergy and other persons who ask for the individual by name. We proposed to add the words "use or" to this permission, to cover the provision of such information to clergy who are part of a facility's workforce.

3. Section 164.510(b)(3) covers uses and disclosures of protected health information when the individual is not present to agree or object to the use or disclosure, and, as pertinent here, permits disclosure to persons only of "the protected health information that is directly relevant to the person's involvement with the individual's health care." We proposed to delete the last two quoted words and substitute the following: "care or payment related to the individual's health care or needed for notification purposes." This change aligns the text of paragraph (b)(3) with the permissions provided for at paragraph (b)(1) of this section.

4. Where an employer needs protected health information to comply with workplace medical surveillance laws, such as the Occupational Safety and Health Administration or Mine Safety and Health Administration requirements, § 164.512(b)(1)(v)(A) permits a covered entity to disclose, subject to certain conditions, protected health information of an individual to the individual's employer if the covered entity is a covered health care provider "who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer." We proposed to amend the quoted language by removing the words "who is a member of the workforce of such employer or," as the language is unnecessary.

5. At § 164.512(k)(1)(ii), we proposed to replace the word "Transportation" with "Homeland Security." The language regarding a component of the Department of Transportation was included to refer to the Coast Guard; however, the Coast Guard was transferred to the Department of Homeland Security in 2003.

6. At § 164.512(k)(5), which permits a covered entity to disclose to a correctional institution or law enforcement official having lawful custody of an inmate or other individual protected health information about the inmate or individual in certain necessary situations, we proposed to replace the word "and" after the semicolon in paragraph (i)(E) with the word "or." The intent of § 164.512(k)(5)(i) is not that the existence of all of the conditions is necessary to permit the disclosure, but rather that the existence of any would permit the disclosure.

Overview of Public Comments

One commenter requested clarification about whether business associates may participate in an organized health care arrangement (OHCA) under § 164.506(c)(5). Another commenter recommended against changing the language of § 164.506(c)(5), arguing that such a change could bring entities like employers and pharmaceutical companies into OHCAs that should not otherwise have access to protected health information, and suggested that the Department change the language to make clear that an OHCA may include only professional staff members.

Final Rule

The final rule implements the technical, conforming, and clarifying changes as proposed. In response to the comments regarding which entities may participate in an OHCA, we clarify that a covered entity participating in an OHCA or the OHCA itself may contract with a business associate to provide certain functions, activities, or services on its behalf that involve access to protected health information, provided the applicable requirements of §§ 164.502(e), 164.504(e), 164.308(b) and 164.314(a) are met. Further, the definition of an organized health care arrangement (OHCA) at § 160.103 includes a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. We modified § 164.506(c)(5) as discussed above in recognition of the fact that not all participants in a clinically integrated care setting may be covered entities (e.g., hospital with physicians with staff privileges that are not workforce members). Such change does not permit employers and pharmaceutical representatives to receive access to protected health information from or through an OHCA in a manner they would otherwise be prohibited from now.

V. Modifications to the Breach Notification Rule Under the HITECH Act

A. Background

Section 13402 of the HITECH Act requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information. In some cases, the Act requires covered entities also to provide notification to the media of breaches. In the case of a breach of unsecured protected health