October 2012

Connecting Healthcare with Legal Excellence℠

Health Law Diagnosis

WORKFORCE ACCESS TO PERSONAL PHI AND FAMILY PHI FROM THE COVERED ENTITY'S ELECTRONIC HEALTH RECORD

This edition of Health Law Diagnosis examines whether employees have a right to access their own medical information maintained by a Covered Entity in an electronic health record (EHR). The issue is analyzed under the scope of **access rights** granted to individuals under the Health Insurance Portability and Accountability Act of 1996 and its related Privacy Rule and Security Rule (collectively, "HIPAA"), and as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), as well as those policy considerations implicated where workforce members access their own, as well as family members', health information within a health organization's electronic health records systems (EHRs), as well as in other formats. The question is reviewed and analyzed against the relevant parts of the HIPAA Privacy Rule, as amended by HITECH and its accompanying regulations, as well as Meaningful Use requirements applicable to individuals and access of their health information.

HIPAA

HIPAA restricts uses and disclosures of PHI to those that are specifically permitted by the Privacy Rule, including but not limited to treatment, payment and health care operations, disclosures to the Individual or pursuant to an Individual's authorization, and other limited purposes, such as public health, law enforcement, and as required by law. HIPAA also generally requires that access to and any use or disclosure of PHI be further limited to that "minimum necessary" amount of PHI needed to accomplish the intended purpose or to carry out duties. 45 C.F.R. § 164.514(d).[1]

Access to Own PHI

HIPAA generally provides Individuals with the right to access their health information maintained by a covered entity health care provider ("Covered Entity"). In accordance with 45 CFR 164.524, "an Individual has a right of access to inspect and obtain a copy of health

[1] The minimum necessary standard does not apply to the following: disclosures to or requests by a health care provider for treatment purposes; (ii) Disclosures to the individual who is the subject of the information; (iii) Uses or disclosures made pursuant to an individual's authorization; (iv) Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules. (iv) Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes; and (v) Uses or disclosures that are required by other law.

information about the Individual in a designated record set," excepting certain health information such as psychotherapy notes, information compiled in reasonable anticipation of a civil, criminal or administrative action or proceeding, and certain other health information. A Covered Entity therefore may only deny an individual's request to inspect or obtain a copy of their health information where specifically permitted by HIPAA, including but not limited to where,

- A licensed health care professional has determined, in the exercise of professional judgment, that the *access requested is reasonably likely to endanger* the life or physical safety of the individual or another person;

- The *protected health information makes reference to another person* (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the *provision of access to such personal representative is reasonably likely to cause substantial harm* to the individual or another person.[2]

Information which is not maintained in a designated record set is not subject to HIPAA access rights. Therefore, to the extent certain information within a Covered Entity's EHR systems would not be considered to be part of its designated record set(s), then this information could be excluded when responding to an Individual's request to inspect or have copies of such information provided to him or her.

A Covered Entity ***is permitted*** to require that an Individual submit a request for copies or inspection of their health information **in writing**, as well as the form and format requested by the Individual, if it is readily producible in such form or format, and if not, "in a readable hard copy form or such other form or format as agreed to by the Covered Entity and the Individual."[3] As amended by HITECH, if the Individual requests a copy of their health information in an *electronic form and format,* the Covered Entity must provide it to the Individual where the PHI in question is maintained in an EHR[4] and is readily producible in such form and format.

The Covered Entity must also provide the access in a timely manner, including arranging for a convenient time and place. When denying access, whether in whole or in part, the Covered Entity must make available all other PHI that it does not have grounds to deny, as well as provide the Individual with a written basis for denial.[5] While the minimum necessary standard applies to other uses and disclosures of PHI, it does not apply to disclosures to the

[2] See 45 C.F.R. 164.524(3)).

[3] See 45 C.F.R. 164.522(c)(2).

[4] Note that the HITECH Notice of Proposed Rulemaking, published in 2010, would expand this to PHI maintained in an *electronic designated record set*, regardless of whether it is in an EHR or not. The Final HITECH Rule is awaiting publication currently.

[5] See 45 C.F.R. 164.522(d).

Individual him or herself, nor pursuant to a HIPAA authorization signed by the Individual authorizing a particular use or disclosure.

Therefore, purely for purposes of HIPAA, physicians and other health care providers would *technically* be permitted to access their own PHI maintained within a designated record set whether they are employed by or on the medical staff of Covered Entity. Although a Covered Entity is required under certain circumstances to provide physicians with access to their health information, it is not *required* to provide, nor is prohibited from providing such access, electronically or directly through its EHR systems. Although a Covered Entity must provide health information if readily producible in the form or format requested by the Individual, this would not include blanket access to such information in its EHR and other record systems, and a Covered Entity could treat such requests as it would requests from its patients, and produce the information in an alternative form or format (PHRs, limited "portal" into the EHR system, etc.) as it would for patients and their personal representatives making such requests for access.

Access to Family Members' PHI

HIPAA generally permits disclosure of an Individual's PHI where the Individual has either signed a HIPAA-valid authorization granting the person seeking access permission to do so, or where the person seeking access would be considered the legal representative of the Individual, such as for parents of minors and legal guardians for individuals who are incapacitated. In addition, HIPAA permits limited disclosure of PHI by a Covered Entity to family members without authorization from the Individual, *but only under certain circumstances* where the Individual has had an opportunity to agree or object or in emergency circumstances.

While HIPAA permits uses and disclosures to those who are *involved in the Individual's* care and for notification purposes, **an opportunity to agree or object is required** before information may be disclosed to those family members, relatives or close personal friends of the Individual, or any other person identified by the Individual.[6] Any information so disclosed, however, must be limited to that which is ***directly relevant*** to the person's ***involvement*** with the Individual's care or payment related to the Individual's health care. Any other disclosure to a family member, or access to a family member's PHI by a physician, would be a direct violation of HIPAA.

If the Individual concerning which the physician or other workforce member as a family member or relative is seeking access to their health information is physically present (e.g., is in the Covered Entity currently receiving treatment), then this requires that the Covered Entity:

- Obtain the Individual's agreement;
- Provide the Individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

[6] 164.510(b)(1).

- Reasonably infer from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

Where the Individual is not present (e.g., previously received treatment) or is incapacitated, or there is an emergency,

> "[T]he covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the *best interests of the individual* and, if so, disclose *only the protected health information that is directly relevant to the person's involvement with the individual's health care*. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest *in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information*." (emphasis added).[7]

As such, a physician or other health care provider should ***not*** generally be granted access to a family member's PHI, whether on paper or as maintained electronically within Covered Entity's EHR systems, unless or until the Individual has been provided with the opportunity to agree or object, or as otherwise permitted by HIPAA.

Affording physicians and health care workers with the ability to view not only their own PHI, but the PHI of their family members as well where they are ***not*** the treating physician or otherwise performing a health care or payment operation or other permissible use of PHI under HIPAA, can create potentially a host of unauthorized accesses and "**curiosity viewings**" of patient records of not just direct family members, but other relatives and even "close friends." The HIPAA permissible information which may be disclosed to family members is limited to that which is **"*directly relevant*"** to their role in the Individual's treatment and care and the wealth of information maintained within EHRs may be difficult for direct access by a physician to such information to be so limited. HIPAA also requires generally that disclosures conform to the ***minimum necessary*** to accomplish the intended use or disclosure.[8] By allowing access by a physician or other workforce member to an Individual's EHR, in particular, inadvertent disclosures of information irrelevant to that physician's role in the Individual's care can easily occur more readily than where such records are maintained in traditional forms, as well as intentional unauthorized uses and disclosures.

In sum, HIPAA does not *specifically* prohibit a physician or other health care provider, whether employed or on the medical staff of a Covered Entity, from accessing the health care records of his or her family members receiving or who have received care at Covered Entity's facility and would, in fact, allow disclosure by the Covered Entity under certain circumstances. Nevertheless, as a ***general policy***, access to such information in a Covered Entity's EHRs and other records should be managed through a separate and specific role-based access granted to

[7] §164.510(b)(3).

[8] § 164.514(d)(4).

such staff as an "Authorized Patient Representative" or otherwise only on a case-by-case basis and only after verifying that the Individual has agreed or otherwise has not objected to the access.

Granting Electronic Access to Physicians

As discussed previously, HIPAA does not prohibit a Covered Entity from granting access rights to physicians **to their own PHI** within the various EHRs and other records maintained by the Covered Entity. Therefore, a Covered Entity ***could*** choose to grant access to information *only* within the designated record set (to the extent technically and administratively possible), or could allow access to *all information* it may maintain electronically or otherwise concerning such physician.

However, a Covered Entity is not required to grant such access to PHI directly through its EHR systems and may therefore require, at its discretion, its physicians to utilize the same processes required for patients and their legal representatives to request access to or copies of their PHI, including submitting written requests for such access. This would allow for uniform tracking of access, would ensure access is available only to the designated record set and not the broad array of information now made available within an EHR, as well as provide the opportunity for the request to be reviewed for any circumstances under which disclosure of the information to the patient (i.e., physician) would be detrimental, allowing access to be denied under HIPAA.

For access to PHI of family members where a physician is **not treating the Individual**, a Covered Entity should consider limiting this access on a case-by-case basis, and only after confirming either:

1. that the Individual would not object or otherwise has agreed to allow access to his or her relative or friend who works for or is on the medical staff of Covered Entity AND that the information is limited to that **directly relevant** to the person's role in the Individual's care and treatment; or

2. that the physician is authorized, as a legal representative or pursuant to a HIPAA compliant authorization, to access such information on behalf of or for purposes authorized by the Individual.

While in theory, this scope of access could be limited only by policies and procedures that prohibited access under circumstances other than as identified above, the potential for abuse of "curiosity viewings" and other well-meaning family members, relatives or "close friends" violating HIPAA by accessing their loved-ones health information remains high, and therefore, a Covered Entity may wish to consider requiring compliance with its ordinary processes to allow families access to patient information.

In addition, policies should **prohibit** physicians from making any ***changes, additions, revisions or deletions*** to their own health information maintained in any format by Covered Entity, or the health information of their family members or relatives. This should include audit controls for purposes of ensuring physicians are complying with these policies and procedures.

Likewise, for physicians who seek paper or electronic copies of their health information or the health information of their family members, these should be processed as would a patient's request for copies of his or her health information.

Granting Electronic Access to Other Workforce

Much as discussed with regard to physicians being granted access to their own PHI, and the PHI of their family members, other workforce members technically would also have the same right to access and have copies of their own PHI, in paper or electronic form and format. However, unlike physicians, these individuals' access rights to PHI, particularly within EHRs, may be, from a practical perspective, more restrictive, given HIPAA minimum necessary requirements for access roles, as well as HIPAA Security Rule requirements for access controls and other administrative, physical and technical safeguards. Depending upon how access roles are defined and controlled within the applicable EHR system (e.g., nurses may have access to more limited clinical information than physicians, as would administrative staff, with access only to demographic and financial information), it may not be possible to afford access to the employee's own health record or health record of a family member electronically (i.e., directly through the EHRs) without having to expand the scope of their access rights generally to all other patient health records.

However, for workforce who may have full access to clinical information within the EHRs in general to perform their responsibilities, as long as that access to and use and disclosure of such information complies with the Covered Entity's policies and procedures, then it would not be unreasonable to also permit such healthcare employees to access their own PHI electronically, as well as records of their family members in accordance with the same processes described above for a physician's accesses. For any workforce member who would not have access or be permitted to access patient records in the ordinary course of their duties, any accesses to their own PHI or the records of their family members would need to go through Covered Entity's processes for all other patient requests or requests from their family members.

Meaningful Use and Patient Access Rights

The Medicare and Medicaid Electronic Health Record (EHR) Incentive Program was enacted as part of HITECH to accelerate the growth and adoption of health information technology (HIT) among health care providers as well as provide for standardization and uniformity in the technology itself by promoting "meaningful use" of certified EHR technology (hereinafter, simply "Meaningful Use" or "MU"). For an eligible Covered Entity to participate in, and quality for Meaningful Use incentive payments, they are required to meet certain sets of objectives and their accompanying measures, as well as meet certain other threshold eligibility requirements depending on their participation in Meaningful Use for Medicare, Medicaid, or both. MU contemplates three "Stages," with each Stage building upon the infrastructure and technological functions established by the previous. Currently, Meaningful Use is in Stage 1 for all eligible Covered Entitys and eligible professionals, with Stage 2 requirements having been proposed as of March 7, 2012.

Each Stage requires meeting a set of "mandatory" or **core objectives** and their associated measures as well as a set of "flexible" or **menu set objectives**, of which an eligible Covered Entity must meet five (5) out of ten (10). All core objectives and chosen menu set objectives must be met within the applicable EHR reporting period in order for an eligible Covered Entity (or eligible professional) to be considered a "meaningful user" of certified EHR technology and therefore eligible for incentive payments. In Stage 1, the applicable EHR reporting period is 90-days, with the applicable reporting period for each subsequent year of Meaningful Use demonstration being 365-days.

Stage 1 core objectives for Covered Entitys require, among others, that patients be afforded with access to electronic copies of their health information and electronic copies of their discharge instructions. Specifically, this core measure requires that any patient ***making a request*** *for or being discharged within the applicable reporting period* (e.g., 90 days or 365 days) is provided with an electronic copy of his or her health information or discharge instructions. The applicable measure for electronic copies is: more than 50 percent of all patients of the inpatient or emergency departments who request an electronic copy are provided such copy with one within **three (3) business days** of the request. For electronic discharge instructions, they must be provided at the time of discharge to more than 50 percent of all patients of the inpatient or emergency departments who request such.[9]

The MU objective "provide electronic copies of health information" applies to *any patient requesting specifically electronic copies of his or her health information during the applicable reporting period*, regardless of whether he or she was a patient in the Covered Entity inpatient or emergency department during that timeframe. In order to meet this objective, access should be granted in accordance with the scope of an Individual's rights of access under HIPAA. The Preamble to the Final Rule for the EHR Incentive Program specifically noted that this objective was not meant to conflict with or override HIPAA through meaningful use requirements. Information which must be provided electronically to meet the objective is limited to that of the patients which is maintained electronically in or accessible from the certified EHR technology. Meaningful Use also permits withholding information from the electronic copy to the extent it would be permitted to do so by HIPAA at 45 C.F.R. 164.524, but otherwise requires the Covered Entity provide all of the health information it has available electronically, in accordance with requirements at 45 C.F.R. 170306(d) for EHR technology to be certified.

It is worth pointing out that for Stage 1, at least under the current regulations, only ***electronic copies*** must be provided, ***not*** *electronic* ***access***. Therefore, a Covered Entity may restrict access to its certified and uncertified EHR systems by physicians, nurses and other health care professionals seeking to access their own health information, or the health information of their family members without jeopardizing its potential ability to otherwise meet this particular MU core objective for Stage 1. Otherwise, electronic copies would still need to be provided to any employee requesting such an electronic copy, which must be in a form and format that is human readable and in compliance with HIPAA at 45 C.F.R. 164.524(c).

[9] As this Legal Memorandum focuses on the grant of access to health information by patients and other Individuals, the Meaningful Use requirements for electronic copies of discharge instructions is not discussed in detail.

While the electronic copy may be made available in *any reasonable electronic media* chosen by the Covered Entity (e.g., CD, USB drive, patient portal, PHR), a Covered Entity is required by HIPAA to make *reasonable accommodations* for patient preferences as set forth in 45 C.F.R. 164.522(b).

Although ***electronic access*** to health information in a Covered Entity's EHRs is not required *currently* for purposes of Meaningful Use, such a requirement may potentially be forthcoming for Stage 2 of Meaningful Use. In a Notice of Proposed Rulemaking published on March 7, 2012, proposed Stage 2 requirements were set forth by CMS and ONC regarding modifications to and additional requirements for Meaningful Use objectives and measures. Included in these proposed Stage 1 requirements is that Covered Entitys *must* provide patients the ability to **view online, download**, and **transmit** information about a Covered Entity admission within **36 hours of discharge**. This would mean that a Covered Entity must make available the health information of at least 50 percent of its patients within such timeframe through an online portal or other similar mechanism.

As currently proposed, however, this would not require Covered Entitys to provide patients with the ability to view online, download and transmit information through any particular mechanism (e.g., could offer a full PHR, or choose to offer only a limited online portal through which the required health information which would be made available). As such, a Covered Entity would likewise not be *required* by Meaningful Use in Stage 1, as currently proposed, to grant direct access by workforce members to their own PHI with its EHR systems, and could provide access to any such health information through alternative mechanisms. Likewise, for purposes of Stage 2, this requirement would only apply to patients actually seen or admitted during the applicable EHR reporting period, as it would require the information provided within three (3) days of discharge, rather than after their request.

* * * *

For more information, please contact:

Krystyna Monticello, Esq.
Partner at Oscislawski LLC
tel: 609-385-0833, ext. 2
kmonticello@oscislaw.com

OR

Helen Oscislawski, Esq.
Principal at Oscislawski LLC
tel: 609-385-0833, ext. 1
helen@oscislaw.com

Attorneys at Oscislawski LLC is a health law firm with its main office located in Princeton, New Jersey but a nationwide reputation for experience with and understanding of federal and state privacy and security laws, as well as electronic health information exchange, health information technology, and managing health data breaches. Our attorneys also advise clients on wide-range of other legal issues. For more information about our firm visit www.oscislaw.com. ***For excellent compliance information, tools and solutions, please also visit our affiliated blog & resource website*** *www.legalhie.com.*