Connecting Healthcare with Legal Excellence℠

Health Law Diagnosis

GRANTING CARE COORDINATOR'S ACCESS TO ePHI UNDER HIPAA

This edition of Health Law Diagnosis addresses the scope of access for performing health care operations and related activities using aggregated Protected Health Information ("ePHI") *across* health care providers. Specifically, this summary addresses the extent to which certain third-party care coordinators ("Care Coordinators") may have access to an aggregated database of provider PHI ("Aggregated Data") to perform *treatment activities* and/or *care coordination* and *case management* for one or more health care providers. Aggregated Data generally includes PHI and other data contributed by a variety of health care providers, which may or may not be affiliated with or part of the same healthcare system or organization.

Many health care providers seek to benefit from the wealth of Aggregated Data to perform Treatment and/or Health Care Operations (HCO) activities on benefit their practices and patient populations. Data which is aggregated through a Health Information Exchange Organization (HIO) or through an Electronic Health Record (EHR) can be a valuable tool for providers to ensure patients receive appropriate follow-up care and treatment, identify trends in their patient population, and perform quality improvement and assessment activities, among others, as well as for Accountable Care Organization (ACO) activities. Increasingly, providers and health plans are turning to the use of employed or third-party Care Coordinators to perform these types of activities using Aggregated Data.

The Health Insurance Portability and Accountability Act (HIPAA) permits uses and disclosures for HCO purposes in addition to Treatment purposes under certain circumstances between providers. However, state law restrictions governing hospitals and health care providers generally restrict disclosure of patient information for HCO and other purposes without patient approval. In addition, state laws also restrict use and disclosure of certain sensitive information. Therefore, state laws are dispositive on the extent to which and for what purposes Care Coordinators may access Aggregated Data without patient approval.

HIPAA

Treatment and Payment Activities

HIPAA permits, *but does not require*, uses and disclosures of PHI for **Treatment purposes** of one or more health care providers, including,

> "the provision, coordination or management of health care and related services…, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."[1]

Uses and disclosures are also permitted for Payment purposes among one or more health care providers, including activities taken to obtain or provide reimbursement for the provision of health care, and eligibility or coverage determinations.[2] Where use or disclosure is permitted for Treatment or Payment activities, a covered entity may, but is not required to, obtain consent from the patient. A HIPAA Authorization is not required.

Health Care Operations Activities

HIPAA permits, *but does not require*, uses and disclosures of PHI for **HCO purposes** of the covered entity itself, *as well as* for the HCO activities of another covered entity, **where**:

- Both covered entities have or had a relationship with the patient whose PHI would be used or disclosed;
- The PHI pertains to that relationship; **and**
- The access is for one of the following HCO purposes:
    1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; **or**
    2. Reviewing the competence or qualifications of its own health care professionals, evaluating its own practitioner and provider performance, conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities; **or**
    3. Healthcare fraud and abuse detection or compliance.

45 C.F.R. 164.506(c)(4). Therefore, HIPAA permits PHI to be shared between two covered entities for HCO purposes in accordance with the above conditions.

[1] 45 C.F.R. 164.501.
[2] Id.

OHCA Activities

In certain circumstances, covered entities may also share PHI for HCO activities *even if they do not share a relationship with the same patients*. In an Organized Health Care Arrangement (OHCA), covered entities may share PHI ***for the HCO activities of the OHCA*** between and among the other covered entities participating in the OHCA.[3] The classic example of an OHCA is physicians on the medical staff of a hospital, whereby clinically integrated care is provided.

In order to establish that an OHCA exists, an arrangement must fall into one of the following "types" of activities:[4]

- A clinically-integrated care setting, in which individuals typically receive health care from more than one health care provider; **OR**

- An **organized system of health care** in which more than one covered entity participates, and in which the participating covered entities:

    1. Hold themselves out to the public as participating in a ***joint arrangement***; and

    2. Participate in ***joint activities*** that include at least one of the following:

        - **Utilization review**, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; OR

        - **Quality assessment and improvement activities**, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; OR

        - **Payment activities**, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

For example, established ACOs participating in the Medicare Shared Savings Program could meet the definition of an OHCA for purposes of HIPAA.[5] As such, information may potentially be shared among the ACO's participating health care providers and health plans ***for the* ACO's (/OHCA's) HCO activities**. In such case, access to Aggregated Data would not be limited to those patients whom the covered entities share a treating relationship with, but rather, Aggregated Data may be accessed for any patient enrolled in the ACO provided that the access was to further the HCO activities of the ACO.

---

[3] 164.506(c)(5).

[4] There are three other "types" of OHCAs described by HIPAA; however, the remaining three relate specifically to health plans and insurers and so are not discussed herein.

[5] CMS has also indicated that ACOs can also be HIPAA Business Associates. As a Business Associate, only the ACO itself may aggregate and access the Aggregated Data of the individual participants, disclosing only de-identified PHI back to the individual ACO participants. 76 Fed. Reg. 19556.

STATE LAW

Disclosures of Health Information

New Jersey's Hospital Licensing rules and Board of Medical Examiner ("BME") rules also govern uses and disclosures of patient health information. "Information in the patient's record" and "professional treatment records" generally may not be disclosed without the patient's "*approval"*. Hospitals are also required to afford patients the right to "confidential treatment of information about the patient,"[6] and information may not be released to anyone "outside the hospital" without the patient's "approval" except in limited situations.[7]

Physicians and other health care providers subject to the BME regulations must "maintain the confidentiality of professional treatment records" and generally may not disclose patient information unless specifically permitted by the BME regulations. For example, a physician must maintain confidentiality of such records, except that he or she may,

> "in the exercise of professional judgment and in the best interests of the patient…*may release pertinent information about the patient's treatment* ***to another licensed health care professional*** who is providing or has been asked to provide treatment to the patient…." (emphasis added).[8]

In addition, to the extent that information would potentially originate from *other types of facilities*, such as ambulatory care facilities, these licensing regulations may also require prior patient approval or consent.[9]

Disclosures of Sensitive Information

New Jersey also affords special protection to certain categories of sensitive information ("**Sensitive Information**") such as HIV/AIDS information, STD related information, or genetic information. For example, the New Jersey AIDS Assistance Act (the "AIDS Act"), N.J.S.A. 26:5C-1 *et seq*., prohibits disclosure of HIV/AIDS identifying information, including diagnosis, treatment and testing, without the individual's "prior written consent", except as otherwise specifically authorized by the AIDS Act.[10] Exceptions to this written consent requirement include, but are not limited to:

- To qualified personnel for **management audits, financial audits or program evaluation** if vital to the audit or evaluation (but only if the identity of the person is not identified in any reports or otherwise disclosed);

---

[6] N.J.A.C. 8:43G-4.1(a)(21).

[7] Id. The patient's approval would not be required, for example, if the patient is t*ransferred to another health care facility*, or the release is *required and permitted by law*, or *pursuant to a third-party payment contract.* Id.

[8] N.J.A.C.13:35-6.5(d).

[9] See generally N.J.A.C. 8:43-13.5(a), and (b); N.J.S.A. 30:13-5 (consent requirements for ambulatory care facilities).

[10] N.J.S.A. 26:5C-7, 26:5C-8.

- To qualified personnel involved in **medical education** or in the **diagnosis and treatment of the person** who is the subject, ***but limited to only*** *personnel who are* ***directly involved*** in medical education or the diagnosis and treatment of the person;

- In all other instances **authorized by State or federal law**.

Other categories of Sensitive Information generally requiring an individual's prior written consent include **genetic information**, **drug and alcohol information** (for certain outpatient and inpatient facilities) and **sexually transmitted disease** related information. HCO activities specifically are not among the types of activities authorized for any disclosures of Sensitive Information without such written consent. Therefore, any HCO activities in which a third party would have access to such Sensitive Information will require the affected patient(s) prior written consent.

Additionally, Treatment related to episodes of care for which minors may independently consent under state law ("Emancipated Care") will require the written consent or approval, as applicable, of the affected minor, rather than his or her parent or guardian, where the minor has independently consented to the provision of such Emancipated Care. Therefore, for example, a disclosure of information received during an episode of Emancipated Care will generally require the minor patient's "approval" prior to its disclosed, and disclosure of any STD related information of a minor will generally require written consent. Information protected by the federal drug and alcohol confidentiality regulations at 42 CFR Part 2, or which is maintained by state licensed outpatient and inpatient drug and alcohol facilities, will also generally require the written consent of the minor to disclose.

Role of Care Coordinators

The role of the Care Coordinators and relationship with the individual providers will dictate, in part, the extent to which Care Coordinators may access Aggregated PHI to perform HCO activities. If the Care Coordinators are part of the *"workforce"* of a provider (i.e., an employee or agent), then any "access" and subsequent "use" of PHI *that originates from the provider* for whom they are a workforce member will generally be permitted for and on behalf of that provider. This would require that the Care Coordinators act ***solely*** at the direction of and under the control of the provider for whom they are acting as a workforce member for. Care Coordinators could not take action independently at the request of another entity without authorization from the provider.

Care Coordinator access to Aggregated Data therefore would be permitted by HIPAA based on this form of workforce relationship with the provider as follows:

- If the Care Coordinators are employed by a provider, in-kind or otherwise, or are the agent of such provider, access and use of Aggregated Data **will generally be permitted by HIPAA:**

    a. For the **Treatment** activities of the individual provider and other health care providers;

b. For the **HCO activities** of the **individual provider**, but only if the Aggregated Data from other providers relates to shared patients; or

c. For the **HCO activities of a clearly defined OHCA**.

❖ Any access to Aggregated Data of *other providers* for HCO purposes (outside of the clearly-defined OHCA) will be limited to *only those patients that the one or more providers share a relationship with.*

- For example, if Providers A, B, and C all treated the same identified patients, but Providers D and E did not, then a Care Coordinator working for Provider D could not access Aggregated Data from Providers A, B, and C for HCO purposes, but Care Coordinators working for Provider A could access Aggregated Data from Provider B and C for HCO purposes, as well as, of course, Provider A's own data.

- Care Coordinators for Providers D and E could *only* have access for HCO purposes to the Aggregated Data of Providers A-C under HIPAA **IF:**

  - the access was related to the HCO activities of an identified OHCA in which Providers A-E each participate;
    OR
  - the affected patients provided a HIPAA Authorization;

    AND:

  - Patient "approval" was obtained for state law purposes, *even if* the access may otherwise be permitted by HIPAA for HCO purposes where two providers share patients or for OHCA purposes.

HIPAA Treatment vs. HCO Activities

Because HIPAA restricts the circumstances under which providers may share PHI for HCO purposes, the purposes for which Care Coordinators may access Aggregated Data depends additionally on whether the intended purpose would be for Treatment or for HCO purposes, in addition to their relationship with the underlying provider(s). For example:

- If the Care Coordinators are assisting providers in the performance of Treatment activities, such as scheduling appointments for follow-up testing or reminding patients to refill their prescriptions, then they would be permitted to access the Aggregated Data of all of the providers in the performance of such Treatment activities.

- If the Care Coordinators are performing HCO activities, such as conducting quality improvement and assessment activities, or certain care coordination activities, then they would only be permitted to access Aggregated Data for patients ***shared*** by the underlying provider and other providers.

- If the Care Coordinators are performing HCO activities related to an OHCA, then they would be permitted to access the Aggregated Data in doing so of any providers who participate in the OHCA.

Although HHS maintains the distinction between Treatment and HCO activities, it acknowledged in the HITECH Final Omnibus Rule that, at times, HCO activities may be difficult to distinguish between activities conducted for Treatment purposes.[11] Treatment and HCO both potentially may *share* the following types of activities, as illustrated by HIPAA provisions governing marketing communications:

- Case management and care coordination;

- Treatment recommendations, therapies, health care providers or settings of care.

However, ***HCO** activities* for case management and care coordination, as well as treatment alternatives, would incorporate those activities that are conducted in a "*population-based" fashion*, rather than patient-specific.[12] Other activities such as quality assessment and improvement activities, outcomes evaluation and development of clinical guidelines, provider evaluations and patient safety activities all fall within the definition of HCO.

HHS has provided guidance in the context of marketing communications in understanding what is "Treatment" vs. "HCO" activities. A communication is not "marketing" where it is made for treatment purposes or for certain HCO purposes (provided no remuneration is received in exchange for making the communication, as amended by HITECH). Although HHS did not specifically discuss or describe types of case management and care coordination activities which would be Treatment or HCO activities, other activities specifically referred to by HHS in distinguishing between Treatment and HCO activities include:

- For HCO activities, promoting health in a general manner and ***population-based health activities,*** including general health promotional mailings, such as reminding women to get an annual mammogram, mailings providing information about how to lower cholesterol, new developments in health care, cancer prevention and health fairs.

- For Treatment activities, to further the treatment of a particular individual's health care status or condition, such as prescription refill reminders to patients, the provision of a free drug sample to a patient, or referral of a patient by his or her primary care physician to a specialist for a follow-up test, or alternative treatments describing ointments, medications and alternative medicine for specific patient conditions.

Therefore, a specific patient record being queried by his or her primary care provider during a follow-up visit after discharge from a hospital may appropriately be characterized as Treatment, whereas patients being queried who are female of a certain age and who have not

[11] 78 FR 5595.

[12] See generally the definition of HCO at 164.501, which states "population-based activities relating to…case management and care coordination, contacting of health care providers and patients with information about treatment alternatives…."

had mammograms for purposes of sending annual mammogram reminders would be appropriately characterized as HCO. As such, **whether and to what extent Care Coordinators may access Aggregated Data of other providers without patient Authorization under HIPAA will depend upon whether the proposed access will be characterized as Treatment or HCO activities of the provider(s).**

Likewise, certain activities being performed within an ACO participating in the Shared Savings Program may qualify as HCO activities or Treatment activities, depending upon whether the ACO itself is performing such activities (and whether it is doing so as a covered entity or a business associate of the covered entity providers) or the individual providers themselves. Additionally, how an ACO is structured will affect uses and disclosures for Treatment and ACO, for example, whether an ACO potentially may qualify as an OHCA through which the individual participating providers may share PHI for HCO purposes of the ACO. An ACO could also qualify as a HIPAA Business Associate of the individual participating providers, to the extent that the ACO is performing HCO activities on behalf of the individual participating providers. If a covered entity in and of itself (i.e., a health system and its affiliated providers operating the ACO), activities conducted by the ACO itself may qualify as Treatment activities, in addition to the other HCO activities conducted by the ACO.

Recommendations and Other Considerations

- ***Define the role and scope of access of Care Coordinators.*** Policies and agreements should specify:

  1. The ***type*** of access (remote; electronic; aggregated etc.);
  2. What ***information*** will be accessed? (selected PHI; aggregaged; everything);
  3. What ***purpose*** (Treatment; HCO of provider; HCO of OHCA);
  4. On ***behalf of whom***? (Provider; OHCA; others?);
  5. Whose ***responsibility*** is it to grant CC's access, oversee, audit and manage?;
  6. Who is ***authenticating*** CC's and checking their authorization, credentials etc.;
  7. How will the scope of access by ***limited by the EMR*** (i.e., firewall "lifted" and ALL records in EMR for ALL practices and hospital are available; or only selected data will be made available to CCs and not the kitchen sink).

- ***State specific considerations.***

  1. State law restrictions generally will apply to any disclosures of patient health information, Sensitive or otherwise, outside of the entity from which it originates or where it is maintained (i.e., access to Aggregated Data of another provider).

2. **Patient approval** for purposes of state restrictions is not strictly required to be in **writing**.

   - Therefore, providers may obtain verbal approval from patients, and potentially even *informal approval*, for example, by **use of provisions in the provider's Notice of Privacy Practices which describe the disclosures** the provider may make of the patient's health information, and by obtaining an "**acknowledgment and approval**" from the patient after receipt of such Notice of Privacy Practices.

   - Approval may also be obtained through written consents signed by patients at Registration by inclusion of provisions that authorize use and disclosure to other entities for the treatment, payment and health care operations of the provider and such third-party entities.

3. As an *alternative* to obtaining patient "approval" or written consent for purposes of *state law*, the Care Coordinators could be designated and **act as the agents** or workforce members of **each and every provider whose Aggregated Data would be accessed and used by the Care Coordinators for HCO purposes.**[13]

   - ***However,*** the purposes for which the Care Coordinators could access Aggregated Data for HCO activities would still be limited by HIPAA as described above.

   - The providers collectively would need to agree upon the direction and control of the Care Coordinators. This would require clear agreement between the providers on the scope and purposes of the Care Coordinators accesses.

   - Care Coordinators would be prohibited from disclosing any Aggregated Data containing Sensitive Information from one provider to another, even though acting on behalf of each.

4. Where consent is expressly required for Sensitive Information, however, this must be in writing, and must generally

   - describe the specific information to be disclosed,

   - list or describe the third party(ies) the information is to be disclosed to, and

   - describe the purpose for which the information is being disclosed.

[13] The obtaining, maintaining and use of **genetic information**, however, will generally require the patient's written consent, *even if* the provider does not disclose the information outside of the facility. N.J.S.A. 10:5-47. Generally, a hospital or other provider's consent form to obtain and maintain genetic information, such as to perform genetic testing, can be drafted to cover internal uses of the genetic information for treatment and related purposes, as well as potentially disclosures to third parties for treatment, payment and HCO purposes.

New Jersey does not specifically prohibit combining a consent for disclosure of Sensitive Information with a consent for disclosure of general health information, nor does HIPAA specifically prohibit a HIPAA Authorization, where required, from being combined with any form of authorization which may be required under State law. However, many hospitals and providers may not routinely obtain comprehensive consents at Registration or otherwise authorizing disclosure of the specific types of Sensitive Information which may be maintained in the provider's records, for the specific purposes a Care Coordinator would access the Sensitive Information for, to such Care Coordinators.

5. Sensitive Information and other patient health information which the patient did not "approve" for disclosure (when required) should be *"flagged"* and restricted from flowing into the Aggregated Dataset, or otherwise *withheld from access* by third parties after contributed to an Aggregated Dataset, a Care Coordinator would be prohibited from access to any Aggregated Data.

6. Because Care Coordinators would have no way of knowing whether Aggregated Data for a given patient would contain Sensitive Information for which written consent to access would be required, prior written consent would need to be obtained before any Care Coordinator was permitted to access the Aggregated Data of any other provider other than the provider for whom the Care Coordinator was acting as a member of its workforce or as an agent.

* * * *

If your organization needs more help understanding how to grant care coordinators access to ePHI in accordance with HIPAA, we can assist. For more information, please contact:

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

OR

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