The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Permitted Uses and Disclosures: Exchange for Health Care Operations

45 Code of Federal Regulations (CFR) 164.506(c)(4)

The Health Insurance Portability and Accountability Act (HIPAA) governs how Covered Entities (CEs) protect and secure Protected Health Information (PHI). HIPAA also provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities *without first obtaining* an individual's authorization: including for **treatment and for health care operations** of the disclosing CE or the recipient CE when the appropriate relationship exists.

Other laws may apply. This fact sheet discusses only HIPAA. Under HIPAA, a CE can disclose (whether orally, on paper, by fax, or electronically) PHI *to another CE or that CE's business associate* for the following subset of health care operations activities of the *recipient* CE (45 CFR 164.501) without needing patient consent or authorization (45 CFR 164.506(c)(4)):

- Conducting quality assessment and improvement activities
- Developing clinical guidelines
- Conducting patient safety activities as defined in applicable regulations
- Conducting population-based activities relating to improving health or reducing health care cost
- Developing protocols
- Conducting case management and care coordination (including care planning)
- Contacting health care providers and patients with information about treatment alternatives
- Reviewing qualifications of health care professionals
- Evaluating performance of health care providers and/or health plans
- Conducting training programs or credentialing activities
- Supporting fraud and abuse detection and compliance programs.

In general, before a CE can share PHI with another CE for one of the reasons noted above, the following three requirements must also be met:

1. Both CEs must have or have had a relationship with the patient (can be a past or present patient)
2. The PHI requested must pertain to the relationship
3. The discloser must disclose only the minimum information necessary for the health care operation at hand.

Under HIPAA's minimum necessary provisions, a health care provider (hereafter "provider") must make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure or request. (45 CFR 164.502(b)). For example, in sharing information with an individual's health plan for population health programs (for example, a diabetes management program), a provider should disclose the PHI that is necessary for the program to be effective.

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

If the CEs are in an "Organized Health Care Arrangement," or "OHCA," as defined in the HIPAA Privacy Rule (45 CFR 160.103), additional capabilities may exist for interoperable exchange of PHI.

The following pages contain example Permitted Uses and Disclosures situations that fall into the health care operations category.

Exchange for Case Management by a Payer

A health plan hires a health care management company to provide semi-monthly nutritional advice and coaching to its diabetic and pre-diabetic members, making the care planning company the health plan's BA. To provide appropriate nutritional advice and coaching, the health care management company needs additional information about the members to make sure the advice is consistent with current treatment received from their medical providers.

The health care management company may query the members' medical providers to obtain information that could impact the nutritional advice being offered. Providers may respond to the query using Certified Electronic Health Record Technology (CEHRT) and may disclose PHI necessary to achieve the case management purpose for which the nutritional coach was hired by the health plan. Disclosure of electronic PHI by CEHRT or other method requires HIPAA Security Rule compliance.

In this scenario, the disclosures by the providers to the care management company (the health plan's BA) are for the health care operations ("population-based activities relating to improving health or reducing costs" and "case management") of the health plan, and therefore are permissible disclosures under HIPAA. A business associate agreement (BAA) is required only between the health plan CE that hires the health care management company BA and that company. The responding CEs may make permissible disclosures directly to the health plan's BA without a BAA between the discloser and the BA (without the need to execute their own BAA with the care management company), just as they could share this information directly with the health plan.

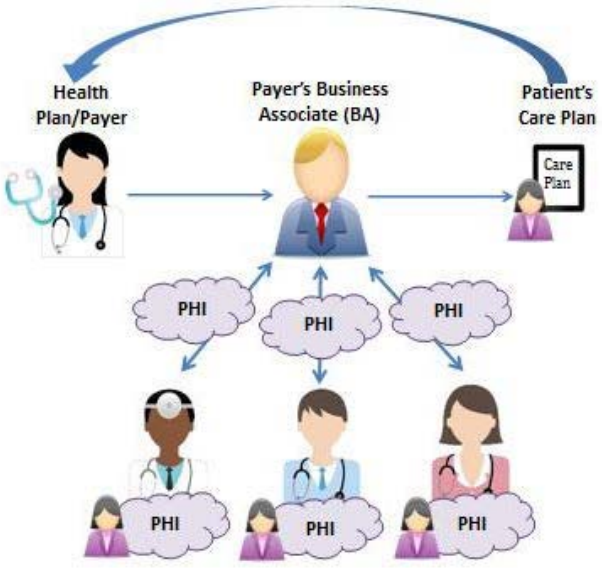

Figure 1: Case Management Scenario

As in the prior scenarios, the providers sharing PHI with the health plan's BA are not responsible under HIPAA for what the BA subsequently does with the information once information has been sent to the BA for a permissible reason and in a secure manner.

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Exchange for Quality Assessment (QA)/Quality Improvement (QI)

There are two examples in this scenario: an ACO quality committee and a quality assessment program using a health information exchange (HIE).

Example 1: ACO Quality Committee

An Accountable Care Organization (ACO) that consists of multiple providers operating as an Organized Health Care Arrangement (OHCA) sponsors a quality committee comprised of individuals who are in the workforce of the providers who operate as an OHCA. The quality committee plans to obtain and review treatment and health outcomes of ACO patients who experienced hospital-acquired infections and surgical errors for the quality assessment and improvement purposes of the ACO/OHCA.

Providers participating in the ACO/OHCA may permit the ACO quality committee to access the PHI needed for the quality assessment through CEHRT.

If the ACO were not operated as an OHCA, or the quality committee was evaluating care quality on behalf of individual providers in the ACO, the providers participating in the ACO could permit the ACO quality committee to access the necessary PHI for the quality assessment through CEHRT, but only for patients whom the requesting and disclosing providers have in common, pursuant to 45 CFR 164.506(c)(4).

Figure 2: QA/QI ACO Scenario

In both instances (OHCA and non-OHCA), access to, or disclosure of, electronic PHI can be made using CEHRT or other method so long as the HIPAA Security Rule is complied with.

Example 2: Quality Assessment using a Health Information Exchange:

As part of a quality review, a provider may need to know the health outcome of a patient that they treated but no longer have contact with (e.g., patient was transferred to another provider). The provider may query a HIE for the relevant health outcomes of the individual.

A provider who has treated the patient and is responding to this query may use CEHRT to send the relevant information to the requesting provider through a HIE. Disclosure of electronic PHI by CEHRT or

other electronic method requires HIPAA Security Rule compliance. This scenario works for any CEs who participate in a health information exchange and is not limited to provider CEs.

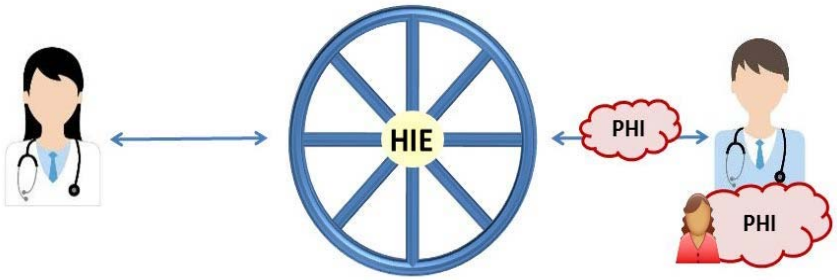

Figure 3: QA/QI Scenario

Quality Improvement Among Several Covered Entities for Population Health

Unaffiliated hospitals in the same community often see the same patients and may not be able to tell whether a patient's hospital-acquired infection resulted from care received at the current treating hospital or from a prior visit to a separate hospital in the community.

The hospitals that have treated or are treating the patient may use CEHRT or a health information exchange to share relevant PHI to try to determine the source for and cause of the infection, so further infections can be prevented.

Disclosure of electronic PHI by CEHRT or other means requires HIPAA Security Rule compliance.

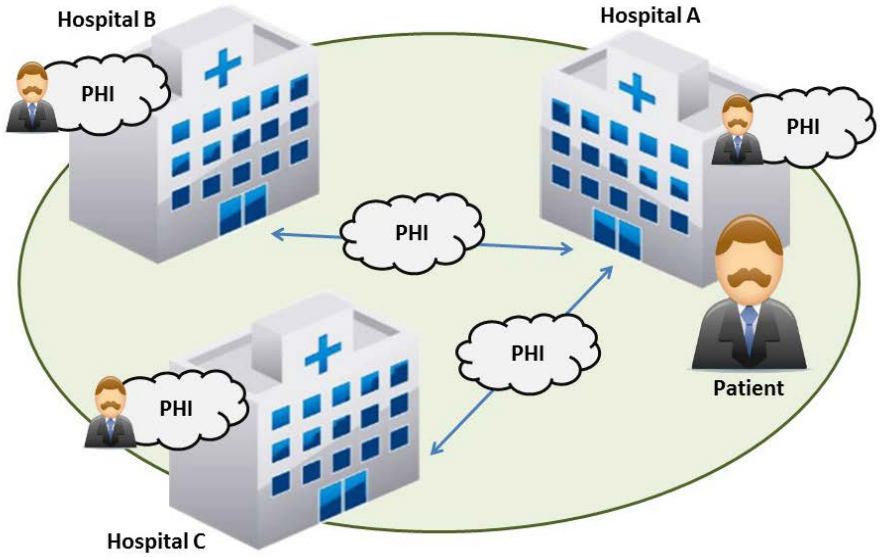

Figure 4: Population-Based Activities Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.