December 18, 2020

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

HIPAA, Health Information Exchanges, and Disclosures of Protected Health Information for Public Health Purposes

This guidance[1] addresses how the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule permits a covered entity or its business associate[2] to use health information exchanges (HIEs) to disclose protected health information (PHI) for the public health activities[3] of a public health authority (PHA).[4]

1. What is a Health Information Exchange (HIE)?

For purposes of this guidance, an HIE is an organization that enables the sharing of electronic protected health information (ePHI) among more than two unaffiliated entities,[5,6] such as health care providers,

[1] This guidance document is not a final agency action and may be rescinded or modified in the discretion of the U.S. Department of Health & Human Services (HHS). Noncompliance with any voluntary standards or suggested practices contained in guidance documents not required by law will not, in itself, result in any enforcement action.

[2] The permissions addressed in this guidance also apply to HIPAA business associates (including health care clearinghouses acting in their role as business associates) to the extent that their uses and disclosures of PHI for these purposes are expressly permitted by their business associate agreements or are consistent with the Office for Civil Rights (OCR) Notification of Enforcement Discretion issued on April 2, 2020 and published in the Federal Register on April 7, 2020. *See* Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19, 85 FR 19392 (April 7, 2020), available at https://www.govinfo.gov/content/pkg/FR-2020-04-07/pdf/2020-07268.pdf.

[3] *See* 45 CFR 164.512(b) (permitting uses and disclosures for certain public health activities and purposes). *See also* https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html.

[4] A public health authority is "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate." 45 CFR 164.501.

[5] This guidance describes such unaffiliated entities as "participants" in the HIE.

[6] *See* 45 CFR 171.102 (definition of "Health information network or health information exchange"), discussed in the preamble to Office of the National Coordinator for Health Information Technology (ONC), Final Rule: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (Cures Act Final Rule). "[T]here must be exchange among more than two unaffiliated individuals or entities besides the HIN/HIE [Health Information Network/Health Information Exchange] that are enabled to exchange with each other. This . . . ensures that the definition does not unintentionally cover what are essentially bilateral exchanges in which the intermediary is simply performing a service on behalf of one entity in providing EHI [electronic health information] to another or multiple entities and no actual exchange is taking place among all entities....." 85 FR 25802 (May 1, 2020). See also 45 CFR 171.103 (definition of "Electronic health information").

health plans, and business associates,[7] for treatment, payment, or health care operations (TPO) purposes.[8] An HIE also may provide other functions and services to its participants (*e.g.*, covered entities, business associates), such as public health reporting to PHAs, patient record location, and data aggregation and analysis.[9] Some examples of HIEs include nationwide and state-wide health information exchanges, regional health information organizations (RHIOs), and some clinical data registries.

2. When does the HIPAA Privacy Rule permit a covered entity or its business associate to disclose PHI to an HIE for purposes of reporting the PHI to a PHA, without an individual's authorization?

The Privacy Rule permits covered entities or their business associates to disclose PHI to an HIE for the HIE to report PHI to a PHA conducting public health activities,[10] in any of the following circumstances:

- ***When the disclosure is required by law.***[11] A covered entity or business associate may disclose PHI to an HIE for public health reporting purposes in accordance with another law (*e.g.*, a mandate contained in federal, state, local, or other law that is enforceable in court) requiring such disclosure.
    - For example, where a state law requires hospitals to transmit patient treatment and laboratory testing data to an HIE for the purpose of reporting to the appropriate state or local public health department, the covered hospital would not violate the Privacy Rule when it transmits the data to an HIE for that purpose.
- ***When an HIE is a business associate of the covered entity (or of another business associate) that wishes to provide PHI to a PHA for public health purposes.*** A covered entity, or a business associate on the covered entity's behalf, may disclose PHI to an HIE that is its business associate in order to transmit PHI to a PHA for the PHA's public health activities. A covered entity or business associate (for or on behalf of a covered entity) may engage an HIE as a business associate to create, receive, maintain, or transmit PHI on the covered entity's behalf for a HIPAA covered function (*e.g.*, for treatment or any other permitted purpose, including public health uses and disclosures).[12]

---

[7] *See* 45 CFR 160.103 (definition of "Business associate").

[8] Other terms that have been used to describe an entity that is an HIE include a Health Information Exchange Organization (HIO) or an HIN. *See also* the preamble discussion in the Cures Act Final Rule about the type of entities that could meet the definition of "Health information network or health information exchange," 85 FR 25642, 25801 (May 1, 2020).

[9] *See* Frequently Asked Question (FAQ) 543, "What may a HIPAA covered entity's business associate agreement authorize a health information organization (HIO) to do with electronic protected health information (PHI) it maintains or has access to in the network?" (December 15, 2008), available at https://www.hhs.gov/hipaa/for-professionals/faq/543/what-may-a-covered-entitys-business-associate-agreement-authorize/index.html

[10] This guidance uses the term PHA to mean a PHA that is authorized by law to collect or receive PHI for public health activities in the circumstances described herein. *See* 45 CFR 164.512(b)(1).

[11] *See* 45 CFR 164.103 (definition of "Required by law").

[12] In accordance with section 13408 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the HIPAA Rules define "Business associate" to expressly include a "Health Information [Exchange] Organization . . . or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." *See* 45 CFR 160.103 (definition of "Business associate," ¶ (3)(i)). A covered entity's business associate also may engage an HIE as a business associate subcontractor. *See* 45 CFR 160.103 (definition of "Business associate," ¶ (3)(iii)).

An HIE acting as such a business associate may disclose PHI to a PHA when the terms of the Business Associate Agreement (BAA) expressly permit or require the HIE to disclose PHI to a PHA on behalf of a covered entity, directly or through another business associate.[13]

In addition, the HHS Office for Civil Rights (OCR) will exercise its enforcement discretion and will not impose penalties on a business associate HIE for disclosing PHI to a PHA during the COVID-19 public health emergency when its BAAs do not authorize the disclosure, consistent with OCR's *Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of PHI by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19* (Business Associate NED).[14]

Examples:

- A covered laboratory[15] may report patient test results (PHI) through an HIE that receives and transmits the PHI to a PHA, when the HIE is performing this data transmission on behalf of the laboratory as the laboratory's business associate.
- A covered laboratory may report patient test results through an HIE that receives and transmits the information to the health care provider that ordered the test for a patient. A health care provider may also use the HIE to transmit the information to a PHA. The HIE may perform both of these data transmissions on behalf of the health care provider as its business associate.
- Consistent with OCR's Business Associate NED, during the COVID-19 public health emergency, an HIE may transmit patient test results it receives in the HIE's role as a covered health care provider's business associate, in response to a PHA's request, regardless of whether the HIE's BAA with the provider permits such disclosure.

- ***When an HIE is acting under a grant of authority or contract with a PHA for a public health activity.***[16] A covered entity, or a business associate acting on the covered entity's behalf (*e.g.*, the covered entity's HIE), may disclose PHI to an HIE that is acting under a grant of authority from, or contract with, a PHA authorized by law to collect or receive such information for public health activities.[17]

---

[13] Sample business associate contract elements are available at https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

[14] *See* 85 FR 19392 (April 7, 2020) and https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf.

[15] HHS addressed when laboratories are covered health care providers in the preamble to the Final Rule on Clinical Laboratory Improvement Amendments (CLIA) Program and HIPAA Privacy Rule; Patient Access to Test Reports. *See* 79 FR 7290, 7291 (February 6, 2014) at https://www.federalregister.gov/d/2014-02280.

[16] *See* 45 CFR 164.501 (definition of "Public health authority"). *See also* the description of public health activities in 45 CFR 164.512(b).

[17] Evidence of a grant of authority could include a written statement on appropriate government letterhead or the PHA's official website that the HIE is acting under the PHA's authority, or could include a contract for services, a memorandum of understanding, a purchase order, or similar documentation that establishes that the person or organization is acting on behalf of the public official. The Privacy Rule does not permit covered entities to disclose PHI to private organizations for public health reasons absent a nexus between the private organization and government public health authority or other underlying legal authority; otherwise, covered entities would have no basis for determining which data collections were "legitimate" and how the confidentiality of the information would be protected. *See* 65 FR 82462, 82547, 82624 (December 28, 2000). *See also* OCR and Office of the Assistant Secretary for Preparedness and Response (ASPR), "HIPAA: Public Health Authority Disclosure Request Checklist," (2014) at https://www.hhs.gov/sites/default/files/hipaa-disclosure-chcklist102314.pdf.

Examples:

- A PHA can engage an HIE to collect laboratory test results from health care providers, regardless of whether the providers are participants in that HIE. A covered laboratory that is not a participant in the HIE is permitted to transmit patient test results to the HIE, for transmission to the PHA.[18]
- A state PHA can engage an HIE to collect test results and associated patient information from health care providers and then transmit that information into the state's electronic contact tracing systems.[19]

Except for disclosures required by law, which must be limited to the relevant requirements of such law,[20] a covered entity generally must make reasonable efforts to limit the PHI disclosed to PHAs to the minimum necessary to accomplish the intended purpose of a public health disclosure.[21] However, a covered entity may rely, if such reliance is reasonable under the circumstances, on a PHA's representations that the PHI it is requesting is the minimum necessary to accomplish the public health purpose of the request.[22]

3. Can a covered entity rely on a PHA's request to disclose a summary record to a PHA or HIE as being the minimum necessary PHI needed by the PHA to accomplish the public health purpose of the disclosure?

Yes. When a PHA requests a summary record or other specified data set, the covered entity may rely, if such reliance is reasonable under the circumstances, on the request being the minimum necessary information the PHA needs for its stated public health purpose if the PHA so represents.[23] In such cases, the Privacy Rule does not require a covered entity to make an independent determination of minimum necessary when responding to a request from a PHA for the PHA's public health activities.

Most health care providers' electronic health record systems (EHRs) are capable of generating a summary record containing a standard set of patient data elements (*e.g.*, the Common Clinical Data Set (CCDS) or United States Core Data for Interoperability (USCDI)).[24] A covered entity may make the PHI in a summary record available to an HIE, or may transmit the record through an HIE to a PHA, if the disclosure to the HIE is required by law, the HIE is a business associate of the covered entity (or a

[18] A PHA also can engage an HIE to use the PHI it collects or receives to conduct public health data analytics, as the Privacy Rule permits a covered entity to disclose PHI to the HIE for this purpose, when the HIE is conducting the activity under a grant of authority from, or contract with, the PHA.

[19] *See, e.g.,* https://coronavirus.maryland.gov/pages/contact-tracing.

[20] *See* 45 CFR 164.512(a)(1).

[21] *See* 45 CFR 164.502(b)(1) and (2)(v).

[22] *See* 45 CFR 164.514(d)(3)(iii)(A).

[23] *See* 45 CFR 164.514(d)(3)(iii)(A). *See also* OCR, FAQs on Minimum Necessary, at https://www.hhs.gov/hipaa/for-professionals/faq/minimum-necessary/index.html.

[24] The USCDI is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange required by the ONC 2015 Edition Cures Act Update. The USCDI replaces the Common Clinical Data Set that was previously required as part of the 2015 Edition health IT certification. *See* ONC, 2015 Edition Certification Companion Guide (February 2, 2018), at https://www.healthit.gov/sites/default/files/topiclanding/2018-04/2015Ed_CCG_CCDS.pdf; and ONC, USCDI (July 2020), at https://www.healthit.gov/isa/sites/isa/files/2020-07/USCDI-Version-1-July-2020-Errata-Final.pdf.

subcontractor business associate through another business associate), or the HIE is acting under a grant of authority from or contract with the PHA for public health activities.

Examples:

A covered hospital, laboratory, or other health care provider may reasonably rely on a PHA's representation that its request for PHI is the minimum necessary information for its stated purpose in the following, and similar, situations:

- The Centers for Disease Control and Prevention (CDC), in its capacity as a PHA, requests that health care providers disclose PHI on an ongoing basis for all prior and current cases of patients exposed to COVID-19, whether suspected or confirmed, using Electronic Case Reporting (eCR), the automated generation and transmission of case reports from EHRs to public health agencies, for review and action.[25]
- A state health department asks all health care providers in the state to report diagnoses of influenza and related patient information using an electronic continuity of care document, a type of summary record that includes patient identity, demographic information, and laboratory test results.[26]
- A local PHA requests that covered health care providers participating in a regional HIE submit summary records with the CCDS or USCDI, such as a Consolidated Clinical Document Architecture Release 2.1 (C-CDA) document, for all patients with COVID-19, using a public health reporting app.[27]

4. May a covered entity disclose PHI to a PHA through an HIE without receiving a direct request from the PHA?

Yes. The Privacy Rule permits a covered entity to disclose PHI through an HIE to a PHA for public health activities, and this permission does not require that the covered entity receive a direct request for PHI from the PHA if the covered entity knows that the PHA is using the HIE to collect such information, or that the HIE is acting on behalf of the PHA.[28] For example, a city health department (a PHA) that is authorized by law to obtain COVID-19 related test results, and to track the overall health of the individuals tested over time, may contract with, or grant authority to, a regional HIE to receive summary records about individuals tested for the virus from local health care providers. A covered

[25] *See* Laura A. Conn and Adi V. Gundlapalli, (CDC), eCR Now: Accelerating Implementation for COVID-19, presentation before the Health Information Technology Policy Committee, April 15, 2020, at https://www.healthit.gov/sites/default/files/facas/2020-04-15_CDC_Presentation_508.pdf; Surveillance Strategy Report — How Sharing Data Digitally Benefits Health, at https://www.cdc.gov/surveillance/innovation/sharing-data-digitally.html; and Information for Health Departments on Reporting Cases of COVID-19, at https://www.cdc.gov/coronavirus/2019-ncov/php/reporting-pui.html.

[26] For example, a state health department may ask health providers to share a patient summary record across a system such as a Patient Unified Lookup System for Emergencies or an HIE to support epidemiological data needs in response to the COVID-19 Pandemic.

[27] For general information about the C-CDA, *see* Implementing Consolidated-Clinical Document Architecture (C-CDA) for Meaningful Use Stage 2, at https://www.healthit.gov/sites/default/files/c- cda_and_meaningfulusecertification.pdf.

[28] *See* 45 CFR 164.512(b)(1)(i) and 164.501 (definition of "Public health authority").

health care provider, acting on its knowledge that the city health department is using the HIE to track COVID-19, may transmit summary records containing PHI for all tested individuals to the HIE for reporting to the city health department, and this disclosure would not violate the minimum necessary standard.

See FAQ 2 for more information about permitted disclosures to HIEs for public health purposes.

5. May an HIE provide PHI it has received as a business associate of a covered entity to a PHA for public health purposes without first obtaining permission from the covered entity?

Yes, during the COVID-19 public health emergency,[29] OCR will not impose penalties on a business associate HIE for violations of certain provisions of the Privacy Rule if the HIE transmits PHI it receives as a covered entity's business associate to a PHA for the PHA's public health activities, regardless of whether the HIE's BAA with the health care provider permits such disclosure or the provider otherwise authorizes the disclosure.

As provided in the Business Associate NED, OCR will exercise its enforcement discretion and will not impose penalties against a business associate or covered entity under the Privacy Rule provisions 45 CFR 164.502(a)(3), 45 CFR 164.502(e)(2), 45 CFR 164.504(e)(1) and (5) if, and only if (1) the business associate makes a good faith use or disclosure of the covered entity's PHI for public health activities consistent with 45 CFR 164.512(b),[30] or health oversight activities consistent with 45 CFR 164.512(d); and (2) the business associate informs the covered entity within ten (10) calendar days after the use or disclosure occurs (or commences, with respect to uses or disclosures that will repeat over time).

- For example, consistent with OCR's Business Associate NED, an HIE that is in a business associate relationship with a covered entity will not be subject to HIPAA penalties if the HIE (1) transmits summary records about individuals diagnosed with COVID-19 to the city health department that is collecting the information to track COVID-19, regardless of whether that public health disclosure is permitted by the HIE's BAA with the covered health care provider; and (2) notifies the covered entity, within 10 days after it first transmitted such information to the city health department, that it is providing such information to the health department.

6. Is a covered entity required to provide notice to individuals about its disclosures of PHI to a PHA for public health purposes? Is an HIE that is a business associate required to provide such notice?

[29] As stated in the published notification, "the [Business Associate NED] will remain in effect until the Secretary of HHS declares that the public health emergency no longer exists, or upon the expiration date of the declared public health emergency (as determined by 42 U.S.C. 247d), whichever occurs first." *See* 85 FR 19392 (April 7, 2020) available at https://www.govinfo.gov/content/pkg/FR-2020-04-07/pdf/2020-07268.pdf.

[30] Accordingly, a business associate may use or disclose PHI consistent with the same conditions that apply to covered entities under 45 CFR 164.512(b), which are described in this guidance. For more information on requirements related to disclosures for public health purposes, *see* https://www.hhs.gov/hipaa/forprofessionals/special-topics/public-health/index.html. *See also* https://www.hhs.gov/hipaa/for-professionals/faq/569/how-may-hipaas-requirements-for-verification-of-identity-be-met-electronically/index.html.

Yes, a covered entity is required to provide individuals with notice that it discloses PHI for public health purposes in the covered entity's Notice of Privacy Practices (NPP). The Privacy Rule requires a covered entity to include in its NPP a description of the purposes, which would include public health purposes, for which the covered entity may use or disclose PHI without an individual's authorization.[31] As such, individuals receive advance notice that their PHI may be used or disclosed for public health purposes when they receive a copy of an NPP, or when they review the covered entity's NPP on its website.[32] In addition, because the Privacy Rule does not require a covered entity to make disclosures for public health purposes, a covered entity may choose to honor an individual's request to *not* disclose PHI about the individual to a PHA, provided that other law does not require the disclosure.

The Privacy Rule does not require a business associate, such as an HIE that is a business associate, to provide individuals with a NPP. However, when individuals request an accounting of disclosures of their PHI, the Privacy Rule requires a covered entity to include an accounting of disclosures (*e.g.,* to a PHA, to the covered entity's business associate) made for public health purposes.[33] In addition, a business associate is directly liable, in certain circumstances, for a failure to provide an accounting of its own disclosures, which would include disclosures of PHI for public health purposes.[34]

Resources

OCR's HIPAA and COVID-19 webpage includes guidance on Disclosures of PHI to Law Enforcement, Paramedics, Other First Responders, and Public Health Authorities at https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html#headingOne.

HHS guidance on laboratory result reporting specified in the Coronavirus Aid, Relief, and Economic Security (CARES) Act, including reporting facilitated by HIEs, at https://www.cdc.gov/csels/dls/locs/2020/hhs_issues_new_cares_act_guidance.html.

Connecting Public Health Information Systems and Health Information Exchange Organizations at https://www.healthit.gov/sites/default/files/FINAL_ONC_PH_HIE_090122017.pdf.

Permitted Uses and Disclosures: Exchange for Public Health Activities at https://www.healthit.gov/sites/default/files/12072016_hipaa_and_public_health_fact_sheet.pdf.

---

[31] *See* 45 CFR 164.520(b)(1)(ii); 45 CFR 164.512(b)(1)(i).

[32] *See* 45 CFR 164.520(c)(3)(i).

[33] *See* 45 CFR 164.528. This general requirement to account for disclosures of PHI does not apply to disclosures of a limited data set for public health purposes pursuant to 45 CFR 164.514(e). *See* 45 CFR 164.528(a)(1)(viii).

[34] See the HITECH Act section 13405(c)(3), 42 U.S.C. 17935(c)(3) ("A business associate included on a list under subparagraph (b) shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting."). OCR plans to issue rulemaking on the accounting of disclosures as required by the HITECH Act section 13405(c)(2).