CONFIDENTIALITY COALITION

GENERAL COMMITTEE MEETING

Thursday, March 19, 2020
3:00 PM to 4:00 PM

Dial-In

888-432-1688; Room**:** 6597; User: 6328

1. **Welcome and Introductions**
2. **ONC Interoperability Final Rule** Attachment 1
3. **CMS Interoperability Final Rule** Attachment 2
4. **Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency** Attachment 3

Office of the National Coordinator of Health Information Technology (ONC) Cures Act Final Rule

Diane Sacks

March 19, 2020

Overview

Implements 21st Century Cures Act provisions

- Updates ONC Health IT Program Certification Requirements
- Establishes Conditions and Maintenance of Certification Requirements for Health IT Developers
- Identifies Reasonable and Necessary Activities that are not Information Blocking

Compliance Dates

- **60 Days after Publication**
  - Certain Health IT Program certifications, including prohibition on restricting certain communications
- **6 Months after Publication**
  - Information blocking prohibitions, but only with respect to EHI represented by the data elements in the USCDI standard
- **24 Months after Publication**
  - Information blocking prohibitions apply to full EHI
  - HL7 FHIR API capability
- **36 Months after Publication**
  - EHI Export capability

Information Blocking Rule

Prohibits certain entities (Actors):

- From engaging - with requisite intent - in a practice likely to interfere with access, exchange, or use of electronic health information (EHI)
- Unless required by law or an exception applies

Actors are:

- Health care providers
- Health IT developers of certified health IT
- Health information exchanges and health information networks (HIE/HINs)

Diane Sacks LLC

Electronic Health Information (EHI)

- Electronic protected health information (as defined in HIPAA)
- To the extent that it would be included in a designated record set (as defined in HIPAA), and
- Regardless of whether the group of records are used or maintained by or for a HIPAA covered entity
- Excludes*:
  - Psychotherapy notes (as defined in HIPAA) or
  - Information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding

***Exclusions are consistent with exclusions for HIPAA access rights**

Diane Sacks LLC

Educating Patients Is Not "Interference"

- May notify patients whether a third-party app developer has attested whether its privacy policy and practices (including security practices) meet certain "best practices" set by the market for privacy policies and practices
- Any information provided to patients must:
  - Focus on any current privacy and/or security risks posed by the app or developer of the app
  - Be factually accurate, unbiased, objective, and not unfair or deceptive, and
  - Be provided in a non-discriminatory manner

Third-Party App Best Practices

- **At a minimum, privacy policies should:**
  - Be publicly accessible at all times, including updated versions
  - Be shared with individuals prior to app's receipt of EHI
  - Be written in plain language and in a manner calculated to inform the individual who uses the app
  - Include a statement of whether and how the individual's EHI may be used or shared, including whether it may be sold at any time (including in the future); and
  - Include a requirement for express consent before the individual's EHI is used or shared, including before it is sold (exceptions for disclosures required by law or necessary as part of sale of the app or a similar transaction)
- **May not prevent an individual from deciding to provide EHI to an app, even if the app does not meet minimum best practices**

Information Blocking Exceptions

- **Exceptions that involve not fulfilling requests to access, exchange, or use EHI**
  - Preventing Harm Exception
  - Privacy Exception
  - Security Exception
  - Infeasibility Exception
  - Health IT Performance Exception
- **Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI**
  - Content and Manner Exception
  - Fees Exception
  - Licensing Exception

Failure to Meet an Exception

- An actor's practice that does not meet the conditions of an exception will not automatically constitute information blocking

- Practices will be evaluated on a case-by-case basis to determine whether information blocking has occurred

Preventing Harm Exception

Harm must be one that could serve as grounds for denial of access under HIPAA Privacy Rule, namely:

- reasonably likely to endanger the life or physical safety of the individual or another person
- reasonably likely to cause substantial harm to another person, or
- access by the personal representative is reasonably likely to cause substantial harm to the individual or another person

Privacy Exception

- Practice must be tailored to the state or federal law precondition
  - For example, cannot require a driver's license to verify identity of a patient when other forms of identification would be permitted under the law
- If state or federal law requires a consent or authorization before disclosing the EHI, the actor must:
  - Use reasonable efforts within its control to provide the individual with a compliant consent or authorization form or provide other reasonable assistance to meet the requirements
  - "Other reasonable assistance" does not require actor to "chase" after individual for valid consent or authorization

Actors Operating Across Multiple States

These actors may adopt uniform privacy policies and procedures to address most restrictive (i.e., most protective) state laws

- Must document approach (uniform policy or state-by-state)
- Cannot apply uniform approach where effect would be to limit an individual's access rights under HIPAA
- Must be implemented consistently and in a non-discriminatory manner
- Repeatedly changing privacy policies depending on the EHI requestor or request could be considered "interference"

Business Associate Agreements (BAAs)

- Some BAAs could have terms that constitute information blocking. For example:
  - If used to discriminate between health care providers
  - If BA with significant market power makes it difficult for a CE to exchange PHI maintained by the BA with others
- ONC would look at negotiations and agreements to determine intent and whether actions constitute “interference”

New Content and Manner Exception

- Not information blocking to limit the content of a response or the manner in which a request is fulfilled
- Allows actors to first attempt to reach and maintain market negotiated terms for the access, exchange, and, use of EHI.
- Content condition may be met with data elements represented in the USCDI standard until 24 months after publication date of final rule
- Manner condition allows fulfillment of request in an alternative manner when (1) technically unable to fulfill the request in any manner requested; or (2) cannot reach agreeable terms with the requestor to fulfill the request.
- Alternative manner must follow specified order of priority and must satisfy the Fees Exception and/or Licensing Exception

Other Privacy Considerations

- **Infeasibility Exception:**

  Not required to fulfill a request where the actor cannot unambiguously segment the requested EHI from other EHI which either may not be shared because of (1) a patient's preference, (2) by law (e.g. Part 2 data) or (3) to prevent harm

- **Fees Exception:**

  Does not allow a fee based in any part on providing electronic access (i.e., that "operates as a toll on electronic access") to an individual, their personal representative, or another person or entity designated by the individual

Compliance and Enforcement

- Enforcement of information blocking civil monetary penalties (CMPs) will not begin until those are established by future notice and comment rulemaking by the Office of the Inspector General (OIG)
- Discretion will be exercised so that conduct before that time is also not subject to CMPs.
- ONC may coordinate reviews of information blocking claims with the OIG, defer to OIG to lead a review, or rely on OIG findings to form the basis of a direct review action
- More information on enforcement will be provided in OIG's future rulemaking

CMS Interoperability and Patient Access Rule

Diane Sacks

March 19, 2020

Time Line

- **6 Months After Publication of Final Rule**
  - Admissions, Discharge and Transfer (ADT) Event Notification
- **Late 2020**
  - Public reporting of information blocking attestations
  - Public reporting of incomplete NPPES information
- **January 1, 2021**
  - Patient Access API
  - Provider Directory API
- **January 1, 2022**
  - Payer-to-Payer Data Exchange
- **April 1, 2022**
  - States Daily Reporting of Dual Eligible Data

Diane Sacks LLC

Patient Access API

To Whom Does It Apply?

Applies to the following CMS-regulated payers (Payers):

- Medicare Advantage (MA) organizations
- Medicaid Fee-For-Service (FFS) programs and CHIP FFS programs
- Medicaid managed care plans and CHIP managed care entities
- Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs), excluding issuers offering only stand-alone dental plans (SADPs) or Federally-facilitated Small Business Health Options Program (SHOP) plans

Patient Access API
What is Required?

Payers must implement and maintain:

- standards-based API that permits third-party applications to retrieve certain data
- with the approval and at the direction of a current individual MA enrollee or the enrollee's personal representative
- without special effort from the enrollee

Diane Sacks LLC

Patient Access API
What Data?

- **Data required to be provided:**
  - **Adjudicated claims**, including claims data for payment decisions that may be appealed, were appealed, or are in the process of appeal, and provider remittances and enrollee cost-sharing pertaining to such claims, no later than one (1) business day after a claim is processed
  - **Encounter data** from capitated providers, no later than one (1) business day after data concerning the encounter is received by the Payer
  - **Clinical data**, including laboratory results, if the Payer maintains this data, no later than one (1) business day after the data is received by the Payer
  - **Outpatient drug data**, including preferred drug lists if applicable and in the case of MA plans offering Part D coverage, formulary data such as tiered formulary structure and utilization management procedures for those drugs

For data maintained by Payer with a date of service on or after January 1 2016

Diane Sacks LLC

Patient Access API
When May Access Be Denied or Discontinued?

Payer may deny or discontinue an app's connection if Payer:

- Reasonably determines, consistent with its HIPAA security risk analysis, that allowing the API to connect or remain connected would present an "unacceptable level of risk" to the security of PHI on the payer's systems; and
- Makes this determination using objective, verifiable criteria that are applied fairly and consistently across all apps and developers used by enrollees, including through criteria that may rely on automated monitoring and risk mitigation tools

Patient Access API
Must Provide Privacy and Security Educational Resources

Payers must provide educational resources in non-technical, simple and easy-to-understand language explaining at a minimum:

- Steps individuals could take to protect the privacy and security of their health information, including factors to consider in selecting an app, secondary uses of the data, and the importance of understanding the security and privacy practices of the app; and
- An overview of which types of organizations or individuals are and are not likely to be HIPAA covered entities, the oversight responsibilities of the Office for Civil Rights (OCR) and the Federal Trade Commission (FTC), and how to submit a complaint to OCR and the FTC

Patient Access API
Must Provide Privacy and Security Educational Resources (cont.)

- Must be provided in an easily accessible location on its public website and through other appropriate mechanisms through which it ordinarily communicates with current and former enrollees

- CMS will provide payers with suggested content they can use and tailor to meet this requirement

Patient Access API
Obtaining Third-Party App Attestations

Payers are allowed, but not required, to request that third-party apps attest that:

- The app has a publicly available privacy policy, written in plain language that has been affirmatively shared with the patient prior to the patient authorizing app access to their health information.
- To “affirmatively share” means that the patient had to take an action to indicate they saw the privacy policy, such as click or check a box or boxes

Patient Access API

Obtaining Third-Party App Attestations (cont.)

May require app to attest that its privacy policy includes, at a minimum:

- How a patient's health information may be accessed, exchanged, or used by any person or other entity, including whether the patient's health information may be shared or sold at any time (including in the future)
- A requirement for express consent from a patient before the patient's health information is accessed, exchanged, or used, including receiving express consent before a patient's health information is shared or sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction)
- If an app will access any other information from a patient's device; or
- How a patient can discontinue app access to their data and what the app's policy and process is for disposing of a patient's data once the patient has withdrawn consent

Patient Access API

Obtaining Third-Party App Attestations (cont.)

- CMS states that payers can look to industry best practices, including the CARIN Alliance's Code of Conduct and the ONC Model Privacy Notice for other provisions to include in their attestation request that best meet the needs of their patient population
- Payer may not discriminate in implementing attestations, such as requiring some apps to provide attestations, but not others

Patient Access API
Apps That Fail to Provide Attestations

- Payer may inform patients if an app did not provide the required attestation
- Notification to the patient should make clear that the app has not attested to having the basic privacy and security protections and indicate what those are, and that the patient should exercise caution before opting to disclose their information to the app
- If the patient still requests the payer make their data available to the third-party app, the payer must provide API access to the app unless doing so would endanger the security of PHI on the payer's systems

CMS Asserts Authority Despite *Ciox Health, LLC v. Azar*

- CMS states that the recent court decision, *Ciox Health LLC v. Azar*, does not affect CMS' "programmatic authorities" to impose the Patient Access API requirements
- In *Ciox*, the court vacated a portion of the HIPAA Privacy Rule that gives individuals the right to direct a covered entity to send PHI that is not in an electronic health record (EHR) to a third party identified by the individual. Under the HITECH Act, individuals only have the right to do this with respect to PHI in an EHR
- CMS notes that because the Patient Access API gives patients access to their own information for their own personal use, it is "consistent with the spirit of access rights under HIPAA"

ADT Notifications Requirements

- While requirement applies only to hospitals that utilize an EHR or other electronic administrative system with certain technical capabilities, but CMS is not specifying any specific method or format for making the notifications
- Hospital has discretion to determine which recipients “need” to receive certain notifications, and may have an intermediary exercise this discretion on its behalf.
- Changed standard to “made a reasonable effort” to send the notifications. This recognizes that some recipients may not be able to receive the notifications, or not in a manner consistent with a hospital system’s capabilities, or that a hospital may not be able to identify provider recipients for some patients.

ADT Notifications
Privacy Issues

- Hospitals will only be required to send notifications if permissible under applicable federal and state law and regulations and "not inconsistent with the patient's expressed privacy preferences
- If a law requires patient consent to send certain information, hospitals would not be expected to share patient information unless they have obtained the consents necessary to comply with existing laws
- Under the "reasonable efforts" standard, a hospital is not required to send a notification when it cannot confirm the identity of a receiving provider
- CMS acknowledges patient matching challenges, but sees that as an "opportunity for the health IT industry to lead the way in developing innovative solutions to patient matching"

Diane Sacks LLC

March 2020

COVID-19 & HIPAA Bulletin
Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency

The Novel Coronavirus Disease (COVID-19) outbreak imposes additional challenges on health care providers. Often questions arise about the ability of entities covered by the HIPAA regulations to share information, including with friends and family, public health officials, and emergency personnel. As summarized in more detail below, the HIPAA Privacy Rule allows patient information to be shared to assist in nationwide public health emergencies, and to assist patients in receiving the care they need. In addition, while the HIPAA Privacy Rule is not suspended during a public health or other emergency, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

In response to President Donald J. Trump's declaration of a nationwide emergency concerning COVID-19, and Secretary of the U.S. Department of Health and Human Services (HHS) Alex M. Azar's earlier declaration of a public health emergency on January 31, 2020, Secretary Azar has exercised the authority to waive sanctions and penalties against a covered hospital that does not comply with the following provisions of the HIPAA Privacy Rule:

- the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care. See 45 CFR 164.510(b).
- the requirement to honor a request to opt out of the facility directory. See 45 CFR 164.510(a).
- the requirement to distribute a notice of privacy practices. See 45 CFR 164.520.
- the patient's right to request privacy restrictions. See 45 CFR 164.522(a).
- the patient's right to request confidential communications. See 45 CFR 164.522(b).

The waiver became effective on March 15, 2020. When the Secretary issues such a waiver, it only applies: (1) in the emergency area identified in the public health emergency declaration; (2) to hospitals that have instituted a disaster protocol; and (3) for up to 72 hours from the time the hospital implements its disaster protocol. When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours have not elapsed since implementation of its disaster protocol.

More on HIPAA Privacy and Disclosures in Emergency Situations

Even without a waiver, the HIPAA Privacy Rule always allows patient information to be shared for the following purposes and under the following conditions.

Treatment Under the Privacy Rule, covered entities may disclose, without a patient's authorization, protected health information about the patient as necessary to treat the patient or to treat a different patient. Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment. See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of "treatment" at 164.501.

Public Health Activities The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information that is necessary to carry out their public health mission. Therefore, the Privacy Rule permits covered entities to disclose needed protected health information without individual authorization:

- ***To a public health authority***, such as the CDC or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability. This would include, for example, the reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR §§ 164.501 and 164.512(b)(1)(i). For example, a covered entity may disclose to the CDC protected health information on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have COVID-19.

- ***At the direction of a public health authority, to a foreign government agency*** that is acting in collaboration with the public health authority. See 45 CFR 164.512(b)(1)(i).

- ***To persons at risk*** of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations. See 45 CFR 164.512(b)(1)(iv).

Disclosures to Family, Friends, and Others Involved in an Individual's Care and for Notification A covered entity may share protected health information with a patient's family members, relatives, friends, or other persons identified by the patient as involved in the patient's care. A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death. This may include, where necessary to notify family members and others, the police, the press, or the public at large. See 45 CFR 164.510(b).

- The covered entity should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object, when possible; if the individual is

incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.

- For patients who are unconscious or incapacitated: A health care provider may share relevant information about the patient with family, friends, or others involved in the patient's care or payment for care, if the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient. For example, a provider may determine that it is in the best interests of an elderly patient to share relevant information with the patient's adult child, but generally could not share unrelated information about the patient's medical history without permission.
- In addition, a covered entity may share protected health information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, for the purpose of coordinating the notification of family members or other persons involved in the patient's care, of the patient's location, general condition, or death. It is unnecessary to obtain a patient's permission to share the information in this situation if doing so would interfere with the organization's ability to respond to the emergency.

Disclosures to Prevent or Lessen a Serious and Imminent Threat Health care providers may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct. See 45 CFR 164.512(j). Thus, providers may disclose a patient's health information to anyone who is in a position to prevent or lesson the serious and imminent threat, including family, friends, caregivers, and law enforcement without a patient's permission. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety. See 45 CFR 164.512(j).

Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification In general, except in the limited circumstances described elsewhere in this Bulletin, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, may not be done without the patient's written authorization (or the written authorization of a personal representative who is a person legally authorized to make health care decisions for the patient). See 45 CFR 164.508 for the requirements for a HIPAA authorization. Where a patient has not objected to or restricted the release of protected health information, a covered hospital or other health care facility may, upon a request to disclose information about a particular patient asked for by name, release limited facility directory information to acknowledge an individual is a patient at the facility, and may provide basic information about the patient's condition in general terms (e.g., critical or stable, deceased, or treated and released). Covered entities may also disclose information when the patient is incapacitated, if the disclosure is believed to be in the best interest of the patient and is consistent with any prior expressed preferences of the patient. See 45 CFR 164.510(a).

Minimum Necessary For most disclosures, a covered entity must make reasonable efforts to limit the information disclosed to that which is the "minimum necessary" to accomplish the

purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.) Covered entities may rely on representations from a public health authority or other public official that the requested information is the minimum necessary for the purpose, when that reliance is reasonable under the circumstances. For example, a covered entity may rely on representations from the CDC that the protected health information requested by the CDC about all patients exposed to or suspected or confirmed to have COVID-19 is the minimum necessary for the public health purpose. In addition, internally, covered entities should continue to apply their role-based access policies to limit access to protected health information to only those workforce members who need it to carry out their duties. See 45 CFR §§ 164.502(b), 164.514(d).

Safeguarding Patient Information

In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information.

HIPAA Applies Only to Covered Entities and Business Associates

The HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity's or business associate's workforce. Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more covered health care transactions electronically, such as transmitting health care claims to a health plan. Business associates generally are persons or entities (other than members of the workforce of a covered entity) that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting protected health information. Business associates also include subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate. The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired). There may be other state or federal rules that apply.

Business Associates

A business associate of a covered entity (including a business associate that is a subcontractor) may make disclosures permitted by the Privacy Rule, such as to a public health authority, on behalf of a covered entity or another business associate to the extent authorized by its business associate agreement.

Other Resources

The COVID-19 Public Health Emergency declaration is available at:
https://www.phe.gov/emergency/news/healthactions/phe/Pages/default.aspx

For more information on COVID-19, please visit: https://www.coronavirus.gov

For more information on HIPAA and Public Health, please visit: https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html

For more information on HIPAA and Emergency Preparedness, Planning, and Response, please https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html

General information on understanding the HIPAA Privacy Rule may be found at: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

For information regarding how Federal civil rights laws apply in an emergency, please visit: https://www.hhs.gov/civil-rights/for-individuals/special-topics/emergency-preparedness/index.html