Advancing SDOH Interoperability: Enabling Privacy and Consent through Standards and Implementations Webinar

Part 1 Questions and Answers

Question	Answered By	Answer*
For ONC CURES, does the patient have to have the ability to decide which diagnoses they want shared and which they do not	Johnathan Coleman	The DS4P standard allows a provider to tag a Consolidated-Clinical Document Architecture (CCDA) document with privacy metadata that expresses the data classification and possible redisclosure restrictions placed on the data by applicable law, such as for 42 CFR Part 2. Currently, it is the combination of applicable law and jurisdictional policy which determine which information is tagged.
Given these descriptions of security tags, how should privacy practices and consent forms be updated to reflect this, and at what juncture should this be discussed with the patient (eg, provider to patient during referral, or front office during after summary care, etc)?	Johnathan Coleman	Data tagging is a technical means to help implement these various disclosure policies, but as a standard, is in itself policy agnostic.
Specifically, if they want to approve their diabetes be shared but not alcoholism? Or can they just say all diagnoses or none?	Josh Mandel	When it comes to individuals sharing records with an app of their choice, ONC's final rule requires that EHRs support SMART on FHIR. This allows users to grant permissions based on FHIR resource types (e.g., "all conditions in my record" or "all observations in my record") but not at the level of finer-grained sets (e.g., "omit my diabetes history" or "omit data from 2019"). EHRs *may* provide additional capabilities for patients to filter or restrict in these ways, but it's not part of the required functionality. In SMARTv2, we're laying groundwork to standardize these kinds of restrictions, but there are significant technical challenges here, since data in an EHR aren't always well categorized in the first place
Is it possible to block specific detail information from being accessed from a broad search but allow it to be accessed for a narrow search. ie vital statistics search will not show blood pressure but a request for blood pressure history would allow it	Josh Mandel	The FHIR API semantics don't really provide for this; it's not so much about authorization as safety. Having Observations *sometimes* held back even though your query requested them and you're authorized to see them... is a recipe for confusion. A safer pattern would be to perform your "broad search" with explicit restrictions (e.g., adding ?_security= with sensitivity levels, or adding a list of Observation codes you want)
During the USCDI security presentation, a potential use case was test results that could be emotionally harmful to a patient. However, ONC guidance in the Information Blocking FAQs states it would likely be interference if an actor "imposed delays on the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results." Could you please clarify this discrepancy?	Kathleen Connor	Response: There is no discrepancy. The citation was to the Preventing Harm Exceptions, which specify when such a delay would *not* implicate Information Blocking. Under the Information Blocking Privacy Exception, per §171.201, an actor who reasonably believes a practice will substantially reduce a risk of cognizable harm to patient(s) or other natural person(s) may delay release of lab results. I.e., it is an Information Blocking Privacy Exception if a provider, who determines based on professional expertise and on patient specific circumstances, delays the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results. 45 CFR § 171.201 - Preventing harm exception - when will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking? See https://www.federalregister.gov/d/2020-07419/p-2199 *Comments.* Several commenters indicated that providers' current organizational policies call for practices that delay the release of laboratory results so that the patient's clinician has an opportunity to review the results before potentially needing to respond to patient questions, or has an opportunity to communicate the results to the patient in a way that builds the clinician-patient relationship. Some commenters indicated their standard practice is to automatically time-delay release of results in general, with an automatic release at the end of a time period determined by the organizational policy in place to ensure that patients can consistently access their information within the timeframe targeted by relevant measures under the CMS Promoting Interoperability Programs. Commenters requested we clarify whether such practices would be recognized under §171.201 or that we recognize such current organizational policies and practices as excepted from the definition of information blocking.

Response. While we recognize the importance of effective clinician-patient relationships and patient communications, we are not persuaded that routinely time-delaying the availability of broad classes of EHI should be recognized as excepted from the information blocking definition under this exception. Consistent with §171.201(d)(3) as finalized, the harm of which a practice must reduce a risk must, where the practice interferes with the patient's access to their own EHI, be one that could justify denying the patient's right of access to PHI under §164.524(a)(3). Currently, §164.524(a)(3)(i) requires that for a covered entity to deny an individual access to their PHI within the designated record set, the disclosure of that PHI must be reasonably likely to endanger the life or physical safety of the patient or another person.[162] No commenter cited evidence that routinely delaying EHI availability to patients in the interest of fostering clinician-patient relationships substantially reduces danger to life or physical safety of patients or other persons that would otherwise routinely arise from patients' choosing to access the information as soon as it is finalized.

Moreover, we are independently aware, and some comment submissions confirmed, that it is not uncommon to automatically release lab and other findings to patients electronically regardless of whether a clinician has seen the information or discussed it with the patient before the patient can choose to access it electronically. We presume these types of automatic releases would not be the case if patients' accessing their information on a timeframe that is more of their own choosing routinely posed a risk to the life or physical safety of these patients or other natural persons. Thus, we believe that where applicable law does not prohibit making particular information available to a patient electronically before it has been conveyed in another way, deference should generally be afforded to patients' right to choose whether to access their data as soon as it is available or wait for the provider to contact them to discuss their results. Only in specific circumstances do we believe delaying patients' access to their health information so that providers retain full control over when and how it is communicated could be both necessary and reasonable for purposes of substantially reducing a risk of harm cognizable under §171.201(d) (as finalized). Circumstances where §171.201 would apply to such delay are those where a licensed health care professional has made an individualized determination of risk in the exercise of professional judgment consistent with §171.201(c)(1), whether the actor implementing the practice is the licensed health care professional acting directly on their own determination or another actor implementing the delay in reliance on that determination. An actor could choose to demonstrate the reasonable belief required by §171.201(a) through an organizational policy (§171.201(f)(1)) with which the practice is consistent, or based on a determination based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use (§171.201(f)(2)), to rely on a determination consistent with §171.201(c)(1).

Comments. Health care professionals commented that clinical experience indicates a systematic and substantial risk that releasing some patient data through a patient portal or API without first communicating the particular results or diagnosis with the patient in a more interactive venue would pose risks of substantial harm to patients. One example commenters specifically cited was genetic testing results indicating a high risk of developing a neurodegenerative disease for which there is no effective treatment or cure. Commenters recommended that we define this exception to allowing delay of the electronic release of such genetic testing results, as a matter of organizational policy, to ensure patients and their families are not exposed to this information without appropriate counseling and context. One comment indicated that delivery by the clinician of the combined results, counseling, and context is clinically appropriate and consistent with the conclusions of relevant research. Start Printed Page 25843

Response. To satisfy the conditions of §171.201, and actor would have to demonstrate that they held a reasonable belief that delaying availability of information until the information can be delivered in combination with appropriate counseling and context in an interactive venue will substantially reduce a risk of harm cognizable under this exception. An actor could accomplish such demonstration through showing the practice is consistent with either an organizational policy meeting §171.201(f)(1) or a determination based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use meeting §171.201(f)(2). However, for a practice likely to, or that does in fact, interfere with the patient's access to their own EHI (§171.201(d)(3)), the actor implementing these practices must demonstrate a reasonable belief that the practice will substantially reduce a risk of harm to the life or physical safety of the patient. The clinician who orders testing of the sort referenced in the comment would, we presume, do so in the context of a clinician-patient relationship. In the context of that relationship, a licensed health care professional should be well positioned to make determinations consistent with §171.201(c)(1) as to specifically when their patients, or other particular natural persons, would face a risk of harm cognizable under §171.201(d)(3)—or §171.201(d)(1) or (2) if or as may be applicable—if the access, exchange, or use of a particular testing result or diagnosis were to be released electronically before it could be explained and contextualized by an appropriately skilled professional, such as a clinician or a health educator, in real time.

Preventing Harm Exception FAQs (excerpt)

No. Blanket delays that affect a broad array of routine results do not qualify for the Preventing Harm Exception. The Preventing Harm Exception is designed to cover only those practices that are no broader than necessary to reduce a risk of harm to the patient or another person.

As we discussed in the Cures Act Final Rule, a clinician generally orders tests in the context of a clinician-patient relationship. In the context of that relationship, the clinician ordering a particular test would know the range of results that could be returned and could prospectively formulate, in the exercise of their professional judgment, an individualized determination for the specific patient that:

		• witholding the results of the particular test(s) from the patient would substantially reduce a risk to the patient's or another person's life or physical safety ***- or -*** • that witholding the results of the particular test(s) from a representative of the patient would substantially reduce a risk of substantial harm to the patient or another person. Such individualized determinations made in good faith by an ordering clinician, in the exercise of their professional judgment and in the context of the treatment relationship within which they order the test, would satisfy the *type of risk* and *type of harm* conditions of the Preventing Harm Exception. Actors, including but not limited to the ordering clinician, could implement practices in reliance on such determinations and the Preventing Harm Exception would cover such practices so long as the practices also satisfy the other four conditions of the exception. No. The *reasonable belief* condition does not include a requirement that the harm be expected to occur within a particular time period or that the likelihood of the harm be high enough to be considered "imminent." (*See* 45 CFR 171.201(a)). The Preventing Harm Exception's *reasonable belief* condition requires an actor engaging in a practice likely to interfere with a patient's access, exchange, or use of their own EHI to have a reasonable belief that the practice will substantially reduce a risk to life or physical safety of the patient or another person that would otherwise arise from the affected access, exchange, or use.
What default security setting for information if non is requested by the patient. How will the patient know about these security options and be able to verify them.	Kathleen Connor	Response: By "security setting", I think you are referring to "security label", i.e., the metadata on protected health information. A security label is assigned by the health information sender of per applicable policy. Applicable policy may be dictated by law, which may be a law requiring that the sender and possibly receivers comply with a patient's privacy consent directive. The health information sharing policy may also be dictated by the sender's organization. In the case of patient generated or access health information, the patient may set the sharing policy. Typically, a community would need to establish a consensus on how to convey these policies using standard security label "tags", which are the discrete elements in a label representing aspects of the policy being represented. This may be accomplished by developing policy specific security label implementation guides that work with the syntax used to convey the health information, e.g., HL7 Version 2 messages, CDA documents, or FHIR Resources. HL7 is developing the basis for creating policy specific implementation guides for each of the HL7 syntax types. A patient would know about which security labels are used within the patient's exchange ecosystem, such as an HIE, when the communities sharing health information within the exchange ecosystem decide on the security label implementation guides they will adopt. RE your question: "How will the patient know about these security options and be able to verify them?" If an exchange ecosystem adopts security label implementation guides, they will likely establish "conformance" requirements to which exchange participants must comply. Since security labels assigned to health information are intended to be persisted with that content, the patient should be able to request access to their shared information, and would be able to inspect it to determine which security labels were assigned, and therefore, which policies governed the sharing of that information.
When do USCDI tags Level 1 take effect?	Kathleen Connor	Response: That depends on when the Level 1 Confidentiality and Purpose of Use tags meet the USCDI criteria for progressing to Level 2, and then the criteria for being adopted in a next version of USCDI. See the criteria and the approach for progressing the various levels of proposed data classes and elements in the following resources: https://www.healthit.gov/cures/sites/default/files/cures/2020-03/USCDI.pdf https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi#blocktabs-uscdi_data_class_element_list-2
How do you manage security labels meant to restrict sharing in USCDI elements that are required to be exchanged in various federal mandates?	Kathleen Connor	Response: Security labels are managed by the communities involved in exchange as metadata about the rules for sharing with protection. The community must establish consensus on how applicable jurisdictional, organizational, and patient privacy policies are conveyed using interoperable security label terminology in accordance with the syntax rules of the exchanged content standards. Until this happens, it will be up to individual senders to decide how to use security labels to comply with restrictions on exchange required under law. HL7® has security label standards for HL7 Version 2, CDA, and FHIR. The HL7 CDA Data Segmentation for Privacy Implementation Guide (IG) and FHIR Data Segmentation for Privacy IG provide the structure and terminology for information exchanged using these formats. At some point, there may be an IG that provides more details about using the Version 2 security label segments. HL7 Security Work Group is developing a Cross Paradigm US Regulatory Security Labeling IG with multiple examples of security labels for various use cases such as Controlled Unclassified Information (CUI) 42 CFR Part 2 for substance use disorders, HIPAA Right of Access, and Minors' rights to control disclosure of sensitive conditions. This IG will illustrate how such labels can be transformed across HL7 Version 2, CDA, and FHIR. References: Cross Paradigm US Regulatory Security Label IG for CUI, Part 2, and 7332 Structure Cross Paradigm US Regulatory Security Labeling IG PSS

Regarding the use case wherein a provider can hold lab data until they are able to provide it with context... I understand that desire from a clinical perspective, to ensure data are not taken out of context. But I also question the appropriateness of a clinician being able to make that decision unilaterally. Perhaps the patient might want their results as soon as possible. Should our technical privacy infrastructure support (or require) patient input on such decisions?	Kathleen Connor	RE: “Should our technical privacy infrastructure support (or require) patient input on such decisions?” Response: There is policy support for patient input as “a right to have such denials reviewed”, but to date, I don’t know of any technical support for this. See 45 CFR § 164.524 - Access of individuals to protected health information at (3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances: (i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or (iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person. (4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.
Please provide a link to that article referenced	Kathleen Connor	Assuming that this is a request for the citation for the definition of segmentation on slide 3: “**Segmentation** The process of sequestering from capture, access or view certain data elements or “datatypes” (clinical information categories) that are perceived by a legal entity, institution, organization, or individual as being undesirable to share.” Response: Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis Melissa Goldstein
Will ONC/SAMHSA/CMS require/incent the use of these security labels?	ONC	Thank you for your question. HHS is interested in advancing the adoption and use of interoperable security tags; as the question indicates, the use of tags by users of health IT is not required at this time. We believe the use of standards can help to reduce providers’ data handling burdens and better satisfy patients offering an important underpinning of the technology innovations and process adaptations to bring the clinician-patient relationship into the 21st century and will continue to explore options for expanding adoption of the standard in practice.
Do EMRs include the ability to store these types of labels/granular consents at the level needed to support this? or do exchanges need to go through a centralized server to manage this?	Bob Dieterle	Depends on the EMR since there is no certification requirement at the moment. The only “centralized servers” are those associated with HIEs or coordination platforms, if one exists in the community and services provides for documenting patient consent to share
Are there any non emergent instances when consent would not be required?	Bob Dieterle	Exchanges under HIPAA for Treatment, Payment and Operations between covered entities and for minimum necessary exchange from a covered entity with a community based entity (see HIPAA FAQs) for treatment and finally in any non-HIPAA environment unless mandated by federal or state law.
How is FERPA being dealt with?	Bob Dieterle	Our initial focus is on release from a HIPAA covered entity or their Business Associate, FERPA is outside of this initial scope
What happens if "patient policy" conflicts with institutional policy (institution actually *owns* the data)?	Bob Dieterle	That depends on the situation and the policies – cannot make a one size fits all response

FYI ... this website seems to have a certificate error (I can't get to it) https://patientcentricsolutions.com/patientshare	Nancy Lush	The link does work and is secure. The user may have had a problem with their browser. Please try it and let me know if you find otherwise. These are all of the links I referenced: I also added one more link to the UMA WG page. HEART WG Home Page https://openid.net/wg/heart/ ONC HEART Webinar Slides https://www.healthit.gov/sites/default/files/page/2019-05/ONCHeartWebinarCombined.pdf ONC HEART Webinar https://www.youtube.com/watch?v=8wpYVQDvYJI UMA Implementations https://kantarainitiative.org/confluence/display/uma/UMA+Implementations PatientCentricSolutions.com/resources https://patientcentricsolutions.com/resources UMA Workgroup: https://kantarainitiative.org/groups/user-managed-access-work-group/

Can you discuss further the group that may be seeking volunteers. How do I found out more ?	Greg White	Providing contact information for the various organizations that were discussed during this webinar:
		
		• HL7 Security Work Group
		  ◦ Main call is on Tuesdays 3 – 4 PM ET
		  ◦ https://us02web.zoom.us/j/82546740051?pwd=WlZwN3BzMWdOUitXS0tmTjVnOThhUT09
		  ◦ Meeting ID: 825 4674 0051 Passcode: 712852
		• HL7 Patient Care SDOH Clinical Care FHIR IG Work Group
		  ◦ https://confluence.hl7.org/display/GRAV/FHIR+IG+Work+Group+Meetings#FHIRIGWorkGroupMeetings-FHIRIGMeetings
		• HL7 Community Based Care and Privacy (CBCP) Workgroup
		  ◦ Tuesdays 12:00 – 1:00 PM ET
		  ◦ https://us02web.zoom.us/j/89234543086?pwd=anE3djgyQXFYbkFYTEZCNVBPYkVzZz09
		  ◦ Meeting ID: 892 3454 3086 Passcode: 873496
		• HL7 Work Groups Call Information
		  ◦ http://www.hl7.org/concalls/CallDirectory.aspx
		• Kantara User Manager Access (UMA) Work Group
		  ◦ https://kantarainitiative.org/groups/user-managed-access-work-group/
		• Join the Gravity Project
		  ◦ https://confluence.hl7.org/display/GRAV/Join+the+Gravity+Project
		• Join the Protecting Privacy to Promote Interoperability Work Group
		  ◦ Contact Serena Mack at serena.mack@drummondgroup.com
		• Participate or Observe Connectathon Testing
		  ◦ HL7 May 2021 Connectathon SDOH Clinical Care IG Track Report Out with ZeOmega – Aunt Bertha Demo Recording https://hl7-org.zoom.us/rec/play/EODqCguvS1duNorPUHfNREs1hB1hA_HY2RfEzsOgmj1hMm2S7xqncVPtOThBbvO9bAPz4DBpwmnxqP-K.Gt58S4rm5Pn4qEkL?startTime=1621452832000
		  ◦ Upcoming Connectathons
		  ▪ CMS HL7® FHIR® Connectathon, July 20-22, 2021, http://www.hl7.org/events/cms/
		  ▪ HL7 September 2021 FHIR Connectathon Sep 13-15, 2021, http://www.hl7.org/events/index.cfm?showallevents
		  ◦ Consent Management, Decision and Enforcement Services Testing Leads
		  ▪ Duane Decouteau ddecouteau@saperi.io, Mohammad Jafari jafarim@gmail.com
		  ◦ SDOH Clinical Care IG Testing Leads
		  ▪ Bob Dieterle rdieterle@enablecare.us, Corey Smith corey.smith@ama-assn.org, Monique van Berkum Monique.VanBerkum@ama-assn.org

*The answers provided herein reflect only the opinion of the person by whom the question was answered and are not necessarily the opinion of ONC.