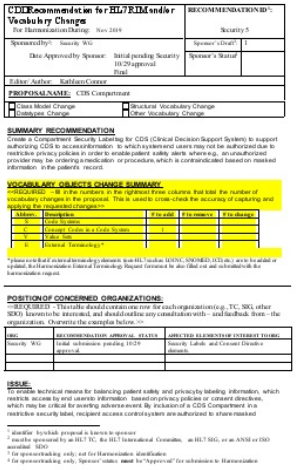
CDS Compartment Proposal November 201911 Harmonization

Proposal 5: CDS Compartment

Create a Compartment Security Label tag for CDS (Clinical Decision Support System) to support authorizing CDS to access information to which system end users may not be authorized due to restrictive privacy policies in order to enable patient safety alerts where e.g., an unauthorized provider may be ordering a medication or procedure, which is contraindicated based on masked information in the patient's record.



CDI Recommendation for HL7 RIM and/or Vocabulary Change

For Harmonization During: Nov 2019

RECOMMENDATION ID*: Security 5

Sponsored By*: Security WG

Date Approved by Sponsor: Initial pending Security 10/29 approval Final

Sponsor vote*: 11

Sponsor's Status*

Editor/ Author: Kathleen Connor

PROPOSAL NAME: CDS Compartment

Class Model Change
Datatypes Change
Structural Vocabulary Change
Other Vocabulary Change

SUMMARY RECOMMENDATION

Create a Compartment Security Labeling for CDS (Clinical Decision Support System) to support authorizing CDS to access information to which system end users may not be authorized due to restrictive privacy policies in order to enable patient safety alerts where e.g., an unauthorized provider may be ordering a medication or procedure, which is contraindicated based on masked information in the patient's record.

VOCABULARY OBJECTS CHANGE SUMMARY

<<REQUIRED — fill in the numbers in the rightmost three columns that total the number of vocabulary changes in the proposal. This is used to cross-check the accuracy of capturing and tracking the requested changes.>>

Abbrev.	Description	# to add	# to remove	# to change
S	Code System			
C	Concept Codes in a Code System	1		
V	Value Sets			
E	External Terminology*			

*please note that if external terminology elements (non-HL7 such as LOINC, SNOMED, ICD, etc.) are to be added or updated, the Harmonization External Terminology Request form must be also filled out and submitted with the harmonization request.

POSITION OF CONCERNED ORGANIZATIONS:

<<REQUIRED — Thereafter should contain one row for each organization (e.g., TC, SIG, other SDO) known to be interested, and should outline any consultation with – and feedback from – the organization. Overwrite the examples below.>>

SIG	RECOMMENDATION APPROVAL STATUS	AFFECTED ELEMENTS OF INTEREST TO SIG
Security WG	Initial submission pending 10/29 approval.	Security Labels and Consent Directive datasets.

ISSUE:

To enable technical means for balancing patient safety and privacy by labeling information, which restricts access by end users to information based on privacy policies or consent directives, which may be critical for averting adverse event. By inclusion of a CDS Compartment in a restrictive security label, recipient access control systems are authorized to share masked

* identifier by which proposal is known to sponsor
* must be sponsored by an HL7 TC, the HL7 International Committee, an HL7 SIG, or an ANSI or ISO accredited SDO
† for sponsor tracking only; not for Harmonization identification
‡ for sponsor tracking only; Sponsor votes must be "Approved" for submission to Harmonization

Document

From CDS 2019-11-13 Meeting Agenda minutes - CDS feedback on the CDS Compartment Proposal

Continued discussion focused on how the provider systems would know to use this label. The use case is within an HIE, satisfying consent use cases where participants have indicated the information can be shared but only in emergency (which averting a patient safety event would fall under emergency). It's still not clear how providers would know whether or not a given data element should be labelled with this.

The gist of this is that most of the use cases so far in CDS usually the access clearance in a particular instance is bound by the access token provided by the client. This is fundamentally trying to change that so that a CDS Server can have broader access and take into consideration that the client requesting the hook is not necessarily authorized to access.

Agree with the use case and intent, but provide the caveat that it will be difficult (if not impossible) in general to understand when to apply this, given that it's not possible in general to determine what data is required for CDS, because the specific CDS algorithms may not be known ahead of time. Committee also provides the feedback that there should be no expectation (and it should be clearly stated as such) that this has to be used in all cases. It should be a specific policy decision to enable use cases in particular environments. Also recognize that this is not the only mechanism to achieve this use case and implementations should be free to choose alternative mechanisms.

From: Kathleen Connor <kathleen_connor@comcast.net>
Sent: Friday, November 1, 2019 12:44 PM
To: 'John Moehrke' <johnmoehrke@gmail.com>; 'Kensaku Kawamoto' <kensaku.kawamoto@utah.edu>
Cc: 'Bryn Rhodes' <bryn@databaseconsultinggroup.com>; 'Guilherme Del Fiol' <guilherme.delfiol@utah.edu>; 'Howard Strasberg' <Howard.Strasberg@wolterskluwer.com>; jenders@ucla.edu; 'Shawn, Christopher A.' <Christopher.Shawn2@va.gov>; 'Trish Williams' <trish.williams@flinders.edu.au>; 'David Pyke' <david.pyke@readycomputing.com>; 'Suzanne Webb' <suzanne.webb@bookzurman.com>; 'Coleman, Johnathan P CTR (US)' <johnathan.p.coleman2.ctr@mail.mil>; 'Alexander Mense' <alexander.mense@hl7.at>; kathleen_connor@comcast.net; 'Mohammad Jafari' <mohammad.jafari@bookzurman.com>
Subject: RE: CDS related Harmonization Proposal

Hi

RE John's statement: "These are indeed uses of the HCS codes, but they are use at the user context, not at the data tagging level."

A CDS Compartment code goes on the information ("data tagging level"), as well. It may be the case that not all information is sent to the CDS controller should be used by a CDS at all times, e.g., in the NV consent and the care team scenario demonstrated at HIMSS where the Share with Protections policy would dictate that a patient's restricted information would not be *used* by the CDS except in the case of an emergency or a potential patient safety issue. That's the difference from what John and Bryn described, where the CDS always has *access*.

A CDS Compartment would prevent an unauthorized provider from breaking the glass or invoking an emergency access unless the CDS recognized a patient safety issue, and then alerts the unauthorized provider. A key use case is for patients with substance use disorders [SUD] being treated by a 42 CFR Part 2 provider.

The Part 2 patient has to consent for e.g., opioid use treatment information to be disclosed to a PDMP or to any provider, in which case the CDS will not know about patient's SUD. While Part 2 permits access to SUD during an emergency, the provider would need to know that the patient has SUD, and know where to find that information if the patient had not consented to disclose it.

A privacy protective patient may prefer to ensure that their SUD is available for patient safety reasons, i.e., Shared with Protections, as is supported by the NV Consent choice #2. The key premise of Share with Protections is to ensure that providers have the information they need when they have a need to know in order to treat a patient safely.

RE Ken's statement: "I would be interested in how the Nevada HIE is planning to actually implement this." The answer for Choice #2: Today, this is likely implemented based on an assertion by the requester that the purpose is an emergency. The HIE would return the patient's information, perhaps with an Emergency purpose of use code.

But without some means for the HIE to have already sent the patient's information for CDS use for patient safety events (labeling the data for CDS Compartment use for patient safety/emergency purposes), the provider would have to check the HIE during the emergency rather than having it already available.

A non-emergency provider, who had queried for patient's information where the patient made consent choice # 2 would not get any information. If that provider had a reason to believe that there's a potential for adverse event, the provider could also assert emergency and access the information. However, a provider that has no inkling of the potential for adverse event may order contraindicated medications/procedures because the technology doesn't support balancing patient privacy with patient safety.

A better approach to Share with Protections would be by implementing security labels on the information that the patient has consented only to be disclosure during an emergency, and permitting the CDS to always have access to it. In the HIMSS demo, the CDS got access to HIE information when the patient was "in context". The HIE would disclose the information for which the patient made NV choice #2 with a security label that has the following HL7 privacy tag codes:

Where the information is HIPAA governed, whether sensitive or not:

- Confidentiality = N (normal)
- Sensitivity = [not specified]
- Policy = HIPAAConsentCD (HIPAA Consent Directive)
- Compartment = CDSCOMPT (CDS compartment)
- Purpose of Use = PATSFTY (patient safety), ETREAT (emergency treatment)

Where the information is sensitive by law, e.g., Part 2

- Confidentiality = R (restricted)
- Sensitivity = SUD or more specifically OPIOIDUD
- Policy = 42CFRPart2 (42 CFR Part 2)
- Compartment = CDSCOMPT (CDS compartment)
- Purpose of Use = PATSFTY (patient safety), ETREAT (emergency treatment)

From Nevada HIE Consent Form (also attached)

The Utah CHIE consent form (attached) also support Share with Protections. A patient must choose a limited opt-in for emergency. Implementation today would likely be similar what I described above for Nevada.

Similarly, NY HealtheLink Consent Form (attached) supports Share with Protections.

Understandably, the notion of "Share with Protections" may be new to some, but it's been a goal for many years, as elaborated in the following:

In 2013, McKinney[1] published a report which proposed a new notion for healthcare: "share with protections."

"Shift the collective mind-set about patient data to 'share, with protections' rather than 'protect.' With the more widespread release of information, the government, leading companies, and research institutions need to consider regulations about its use, as well as privacy protections. To encourage data sharing and streamline the repetitive nature of granting waivers and data-rights administration, it may be better for data approvals to follow the patient, not the procedure. Further, data sharing could be made the default, rather than the exception. It is important to note, however, that as data liquidity increases, physicians and manufacturers will be subject to increased scrutiny, which could result in lawsuits or other adverse consequences. We know that these issues are already generating much concern, since many stakeholders have told us that their fears about data release outweigh their hope of using the information to discovered new opportunities."

Recognizing the concern that "that as data liquidity increases, physicians and manufacturers will be subject to increased scrutiny, which could result in lawsuits or other adverse consequences", HL7 has developed security label syntax for v2, CDA, and FHIR and standard privacy tags (examples shown above) to enable sharing with protections while still respecting patient privacy as described in Mike Davis' paper on the topic.

The purpose of a CDS Compartment code is to enable the CDS to access patient information from the HIE prior to a potential patient safety/emergency to ensure that a provider who has no inkling of potential contraindication or needs the information immediately, has it available in their system. It also ensures that a provider who is not generally authorized to access sensitive information without specific consent will be alerted by the CDS when the patient' s restrictions need to be overridden by Break the Glass.

Thank you again for the opportunity to discuss CDS Compartment proposal.

Best, K

Kathleen Connor

From: John Moehrke <johnmoehrke@gmail.com>
Sent: Thursday, October 31, 2019 7:30 AM
To: Kensaku Kawamoto <kensaku.kawamoto@utah.edu>
Cc: Kathleen Connor <kathleen_connor@comcast.net>; Bryn Rhodes <bryn@databaseconsultinggroup.com>; Guilherme Del Fiol <guilherme.delfiol@utah.edu>; Howard Strasberg <Howard.Strasberg@wolterskluwer.com>; jenders@ucla.edu; Shawn, Christopher A. <Christopher.Shawn2@va.gov>; Trish Williams <trish.williams@flinders.edu.au>; David Pyke <david.pyke@readycomputing.com>; Suzanne Webb <suzanne.webb@bookzurman.com>; Coleman, Johnathan P CTR (US) <johnathan.p.coleman2.ctr@mail.mil>; Alexander Mense <alexander.mense@hl7.at>
Subject: Re: CDS related Harmonization Proposal

These are not data tagging issues. These are context of use issues. The context of the use would differentiate between normal clinical flows, emergency department access, regional emergency declaration (e.g. California fires), and break-glass (i.e. authorized elevation of privilege by medical safety action). These are all distinctions that I have added for clarity. I have no idea which of those this NV policy is referring to with "emergency care". I wonder what the patients think they are authorizing or forbidding. These are indeed uses of the HCS codes, but they are use at the user context, not at the data tagging level. The use of security compartment vocabulary is not always clear, but sometimes these tags are used on data. Most of the time their appearance on the data is implied by the context of the database/system the data are managed within (EHR vs clinical-research database).

John Moehrke Architect: Healthcare Informatics Standards - Interoperability, Privacy, and Security
CyberPrivacy – Enabling authorized communications while respecting Privacy
IHE Co-Chair IT Infrastructure Planning
HL7 Co-Chair Security WG, FHIR FMG, FHIR facilitator, and FHIR Foundation founding member

HITRUST Certified CSF Practitioner
Employee of ByLight Professional IT Services -- Contractor to VHA MyHealtheVet
JohnMoehrke@gmail.com | M +1 920-564-2067 | John.Moehrke@bylight.com
https://www.linkedin.com/in/johnmoehrke | https://healthcaresecprivacy.blogspot.com
Courtney's third law: There are no technical solutions to management problems, but there are management solutions to technical problems.

On Wed, Oct 30, 2019 at 5:05 PM Kensaku Kawamoto <kensaku.kawamoto@utah.edu> wrote:

I would be interested in how the Nevada HIE is planning to actually implement this.

In general, I think this type of a requirement can make life very difficult for a healthcare provider.

Ken

==========

Kensaku Kawamoto, M.D., Ph.D., M.H.S.

Associate Chief Medical Information Officer

Director, Knowledge Management and Mobilization

Vice Chair for Clinical Informatics, Department of Biomedical Informatics

University of Utah

(tel) 801-587-8076

(fax) 801-581-4297

From: Kathleen Connor <kathleen_connor@comcast.net>
Sent: Wednesday, October 30, 2019 3:46 PM
To: 'Bryn Rhodes' <bryn@databaseconsultinggroup.com>; 'John Moehrke' <johnmoehrke@gmail.com>
Cc: Kensaku Kawamoto <kensaku.kawamoto@utah.edu>; Guilherme Del Fiol <guilherme.delfiol@utah.edu>; 'Howard Strasberg' <Howard.Strasberg@wolterskluwer.com>; jenders@ucla.edu; 'Shawn, Christopher A.' <Christopher.Shawn2@va.gov>; 'Trish Williams' <trish.williams@flinders.edu.au>; 'David Pyke' <david.pyke@readycomputing.com>; 'Suzanne Webb' <suzanne.webb@bookzurman.com>; 'Coleman, Johnathan P CTR (US)' <johnathan.p.coleman2.ctr@mail.mil>; 'Alexander Mense' <alexander.mense@hl7.at>; kathleen_connor@comcast.net
Subject: RE: CDS related Harmonization Proposal

Thanks CDS Cochairs for your consideration and feedback.

Heartening to know that generally CDS are given super user access in current systems today, including those that are not able to segment sensitive information for which consent must be given for access. While some sensitive information laws permit use for emergency/avert adverse event scenarios, that's not universal. Maybe the use case for this code needs to be narrowed? Totally open to dropping it as unnecessary.

Wondering how you envision the following Nevada HIE use case to be implemented [See attached Nev HIE Consent Directive]: In Nevada, the HIE can share with recipients only in the case of an Emergency – i.e., not in everyday CDS alerts. [See consent options below.]

I.e., CDS is a super-user if patient selects:

- check box 1 in all circumstances – e.g., suggesting an alternative med/procedure for any end user
- check box 2 only in emergency – i.e., avoidance of potential adverse event (assuming that meets the meaning of an emergency – but if not, there' s a bigger issue)

But is not permitted to act as super user if check box 3?

Seems that some type of flag [security label] on HIE disclosed information would be needed to implement checkbox 2.

Is there some CDS work-around via generalized access control provisioning to deal with this?

<<Nevada HIE Patient-Consent Form.pdf>>

http://pmilv.com/wp-content/uploads/2014/06/HIE-Patient-Consent-Form.pdf

From: Bryn Rhodes <bryn@databaseconsultinggroup.com>
Sent: Wednesday, October 30, 2019 1:47 PM
To: John Moehrke <johnmoehrke@gmail.com>
Cc: Kensaku Kawamoto <kensaku.kawamoto@utah.edu>; Kathleen Connor <kathleen_connor@comcast.net>; Guilherme Del Fiol <guilherme.delfiol@utah.edu>; Howard Strasberg <Howard.Strasberg@wolterskluwer.com>; jenders@ucla.edu; Shawn, Christopher A. <Christopher.Shawn2@va.gov>; Trish Williams <trish.williams@flinders.edu.au>; David Pyke <david.pyke@readycomputing.com>; Suzanne Webb <suzanne.webb@bookzurman.com>; Coleman, Johnathan P CTR (US) <johnathan.p.coleman2.ctr@mail.mil>; Alexander Mense <alexander.mense@hl7.at>
Subject: Re: CDS related Harmonization Proposal

Hi All,

The CDS Work Group discussed this proposal on the call today, and the consensus was that it's not clear how this label could be applied in practice. It would be a significant challenge to identify for every data element whether it was relevant for any potential decision support. More typically, this sort of behavior is implemented with a role that elevates the authorization for a CDS Service as a sort of "super user", which doesn't require labelling of every data element. Further, we would recommend that it be made clear that if this harmonization proposal does get applied, that it doesn't carry any implication of required support within specifications like FHIR and CDS Hooks.

Happy to discuss this issue further, as was suggested earlier in this thread. Perhaps an upcoming CDS WG call? (12:00ET Wednesdays).

Regards,

Bryn Rhodes

bryn@databaseconsultinggroup.com

On Wed, Oct 30, 2019 at 6:42 AM John Moehrke <johnmoehrke@gmail.com> wrote:

I hope that everyone understands that this is what is done today with CDS, they just don't need a HL7 standardized 'compartment' value to do it. This is done today through normal internal access control rules that elevate the CDS service account to have absolute access to data. I am unclear why we need to define a HL7 standardized 'compartment' value, but having it does not mean everyone must switch over to it.

John Moehrke Architect: Healthcare Informatics Standards - Interoperability, Privacy, and Security
CyberPrivacy – Enabling authorized communications while respecting Privacy
IHE Co-Chair IT Infrastructure Planning
HL7 Co-Chair Security WG, FHIR FMG, FHIR facilitator, and FHIR Foundation founding member

HITRUST Certified CSF Practitioner
Employee of ByLight Professional IT Services -- Contractor to VHA MyHealtheVet
JohnMoehrke@gmail.com | M +1 920-564-2067 | John.Moehrke@bylight.com
https://www.linkedin.com/in/johnmoehrke | https://healthcaresecprivacy.blogspot.com
Courtney's third law: There are no technical solutions to management problems, but there are management solutions to technical problems.

On Tue, Oct 29, 2019 at 10:49 PM Kensaku Kawamoto <kensaku.kawamoto@utah.edu> wrote:

Hi Kathleen,

Thanks, that’s helpful.

Is the proposal basically to create a CDS user role, so that this kind of interaction could be supported, but that such support is not mandated? In that case, I think it’s fine to move forward?

Ken

==========

Kensaku Kawamoto, M.D., Ph.D., M.H.S.

Associate Chief Medical Information Officer

Vice Chair for Clinical Informatics, Department of Biomedical Informatics

On Oct 29, 2019, at 9:40 PM, Kathleen Connor <kathleen_connor@comcast.net> wrote:

Hi Ken

Good questions.

You may want to also discuss with Dave Carlson who was the VA lead on the Vignette. I think he summed up the use case very well in the video on Confluence HIMSS 201902 Orlando at the

HIMSS Interoperability Showcase - Consumer Centered Care Planning Use Case Video

Vendors in the Vignette, including Allscripts, were able to share restricted care plan information across the care team. Some care team members did not have access to sensitive information. Since the CDS as a super user was able to access that information, it was able to alert the provider to break the glass. The vendor providing that component used CDS Hooks.

You asked about a proactive CDS use case where a provider who doesn’t know information to which that provider should have had authorized access was able to be informed by the CDS.

That’s a slightly different use case, but very relevant as these are related capabilities. In that case, the provider, who is authorized, would not need to “break the glass” [BTG] to access it.

BTG is invoked where a provider isn’t authorized to access needed information, but is able to invoke BTG because of the risk of adverse event. E.g., a provider who isn’t an Emergency Provider may have a lower level of access to sensitive information, but having a “need to know” overrides the current level of authorization. Usually the system, e.g., VA, will present a warning that this access will be reviewed for appropriateness, so there’s acceptance of accountability by the provider.

Seems like it might be a good idea for CDS/Security/CBDP to hold a join call to go over these areas of mutual interest. Then we can drill down on your community's interest areas more precisely, and make sure that CDS WG is comfortable with this harmonization proposal.

Please let us know if that sounds like a good idea and we'll set up a joint call.

Best, K

Kathleen Connor

VHA Security Architecture – Framework Engineering

Book Zurman Inc.

HL7 Security and Financial Management Cochair

<image001.png>

From: Kensaku Kawamoto <kensaku.kawamoto@utah.edu>
Sent: Tuesday, October 29, 2019 8:04 PM
To: Kathleen Connor <kathleen_connor@comcast.net>; Guilherme Del Fiol <guilherme.delfiol@utah.edu>; 'Howard Strasberg' <Howard.Strasberg@wolterskluwer.com>; jenders@ucla.edu; bryn@databaseconsultinggroup.com
Cc: John Moehrke <JohnMoehrke@gmail.com>; 'Shawn, Christopher A.' <Christopher.Shawn2@va.gov>; 'Trish Williams' <trish.williams@flinders.edu.au>; 'David Pyke' <david.pyke@readycomputing.com>; Suzanne Webb <suzanne.webb@bookzurman.com>; 'Coleman, Johnathan P CTR (US)' <johnathan.p.coleman2.ctr@mail.mil>; 'Alexander Mense' <alexander.mense@hl7.at>
Subject: RE: CDS related Harmonization Proposal

Hi Kathleen,

I don't quite understand the use case. Could you provide a few more examples/scenarios?

Is this something along the lines of –

- An MD, for whatever reason, can't see that a patient is HIV+ (is this even something that's possible in mainstream EHR systems today?)
- The patient is < 65 years, so typically wouldn't be recommended a pneumococcal vaccine
- But because the patient is immunocompromised, the vaccine should be recommended
- So the CDS system in this role recommends the vaccine be given, and asks the user if they want to "break the glass" to see why it's being recommended? Again, is this something that's possible in mainstream EHRs?

Thanks,

Ken

==========

Kensaku Kawamoto, M.D., Ph.D., M.H.S.

Associate Chief Medical Information Officer

Director, Knowledge Management and Mobilization

Vice Chair for Clinical Informatics, Department of Biomedical Informatics

University of Utah

(tel) 801-587-8076

(fax) 801-581-4297

From: Kathleen Connor <kathleen_connor@comcast.net>
Sent: Tuesday, October 29, 2019 8:58 PM
To: Guilherme Del Fiol <guilherme.delfiol@utah.edu>; Kensaku Kawamoto <kensaku.kawamoto@utah.edu>; 'Howard Strasberg' <Howard.Strasberg@wolterskluwer.com>; jenders@ucla.edu; bryn@databaseconsultinggroup.com
Cc: John Moehrke <JohnMoehrke@gmail.com>; 'Shawn, Christopher A.' <Christopher.Shawn2@va.gov>; 'Trish Williams' <trish.williams@flinders.edu.au>; 'David Pyke' <david.pyke@readycomputing.com>; Suzanne Webb <suzanne.webb@bookzurman.com>; 'Coleman, Johnathan P CTR (US)' <johnathan.p.coleman2.ctr@mail.mil>; 'Alexander Mense' <alexander.mense@hl7.at>; kathleen_connor@comcast.net
Subject: CDS related Harmonization Proposal

Dear CDS WG Cochairs,

Ask: For your review and consideration of the attached 201911 Initial Harmonization Proposal.

I'm the vocabulary facilitator for Security and CBCP WGs.

Today, CBCP reviewed and tentatively approved the attached CDS Compartment Harmonization Proposal.

Johnathan Coleman asked that I check with CDS WG for awareness and any feedback you might provide.

Security WG is also interested in getting your input.

Summary

Create a Compartment Security Label tag for CDS (Clinical Decision Support System) to support authorizing CDS to access information to which system end users may not be authorized due to restrictive privacy policies in order to enable patient safety alerts where e.g., an unauthorized provider may be ordering a medication or procedure, which is contraindicated based on masked information in the patient's record.

ISSUE:

To enable technical means for balancing patient safety and privacy by labeling information, which restricts access by end users to information based on privacy policies or consent directives, which may be critical for averting adverse event. By inclusion of a CDS Compartment in a restrictive security label, recipient access control system are authorized to share masked information with a CDS in the event that an unauthorized end user attempts to order a contraindicated e.g., medication or procedure. When triggered, the CDS throws a contraindication alert and advises the end user to "break the glass", e.g., access the masked information in an accountable manner.

Background:

In conjunction with Security WG's Share with Protections work item, we demonstrated the use of security labels to accomplish the above during the HIMSS 201902 Orlando Consumer Centered Care Planning Interoperability Showcase Vignette, with technical details described here: HIMSS 201902 Sharing with Protections

The proposed CDS Compartment label doesn't directly impact a CDS. It does essentially make a CDS a "super user" with authorization to see all healthcare information in order to trigger any pertinent alerts that it may support. It does not in any way stipulate CDS behavior. This is a adjunct to what a CDS may be programmed to do. The intended goal is to balance patient privacy with patient safety where achievable.

Let us know if you have questions, concerns, and feedback. Maybe you've already been thinking along these lines? That would be terrific to find out about.

Best, K

[1] McKinsey & Company, Center for US Health System Reform Business Technology Office, The 'big data' revolution in healthcare, Jan. 2013,