Argonaut Project:
CDS Hooks Security Risk Assessment

Version 1.0

February 26, 2018

Table of Contents

1 Introduction

1.1 Purpose

This document is the final report from a security risk assessment performed with respect to the draft CDS Hooks service specification, at the request of the HL7 Argonaut Project.

1.2 Scope

This security risk assessment identifies risks associated with the CDS Hooks application programming interface (API) that supports synchronous, workflow-triggered clinical decision support (CDS) calls returning information and suggestions to the EHR. The CDS Hooks API is illustrated in Figure 1 below.[1]

Components involved in this API include:

- EHR application (app) that calls a CDS service
- CDS service that performs the action requested by the EHR app and returns one or more "cards" providing information, a suggestion, or a link to an associated app (usually a SMART app)
- Authorization server that receives from an EHR app or CDS service a request for access to FHIR resources, and that, if the access is authorized, returns an access token to the requester
- FHIR resource server that receives from an EHR app or CDS service an access token presented in exchange for the authorized FHIR resources

The specific scope of this security risk assessment includes risks associated with the following exchanges and services, as identified in Figure 1:

1. EHR->CDS: Service calls from an EHR app to a CDS Hooks service (including transmission of a signed JSON Web Token (JWT) for authenticating the EHR app, and transmission of OAuth 2.0 access tokens to CDS Hooks services)
2. CDS->FHIR: CDS services retrieval of FHIR resources from the EHR's FHIR server
3. CDS->EHR: Return of CDS cards from the CDS service to the EHR app
4. Card Services: Services triggered by actionable CDS cards (i.e., suggestion, app link)
5. Web Browser: Web browser vulnerabilities (e.g., Cross-Origin Resource Sharing)

[1] Adapted from CDS Hooks Overview, available from http://cds-hooks.org/ (accessed 1/3/2018).

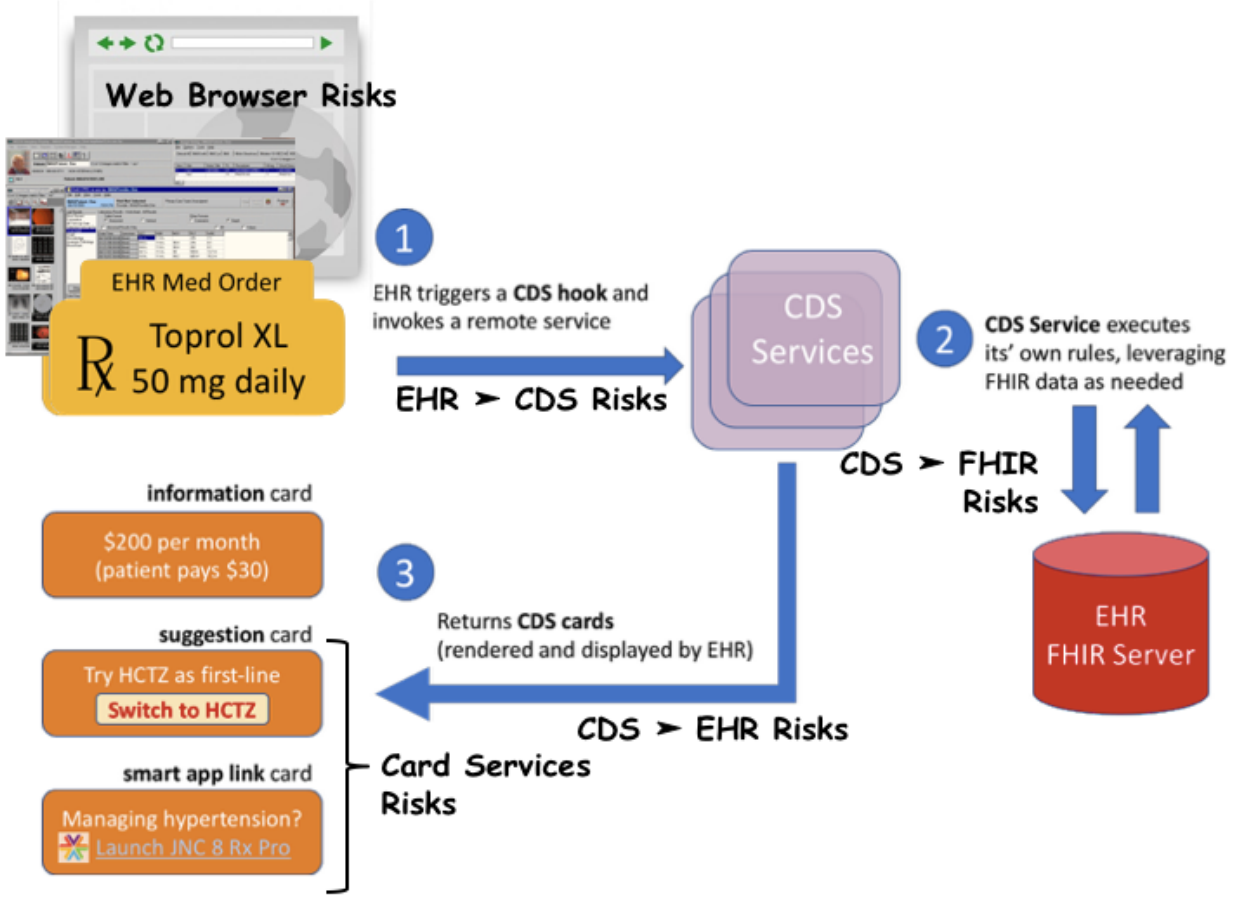

Figure 1. Scope of risks addressed in this security risk assessment.

The scope does not include the OAuth 2.0 authorization process through which the EHR app requests and obtains a bearer token that may be passed on to the CDS service. This process is described, and the API specified, in the SMART App Authorization Guide.

1.3 Assumptions

This security risk assessment makes the following assumptions:

1. A trusted relationship exists among the EHR, the authorization server, and the FHIR server. The EHR app, authorization server, and FHIR server may all be implemented within the same EHR "system" under a single organization, or by multiple systems under different organizations.
2. The CDS service may be implemented and operated by the same organization that operates the EHR, or it may a separate entity.

2 Approach

2.1 Sources

The following sources of information regarding CDS Hooks were used:

- CDS Hooks Overview, http://cds-hooks.org
- CDS Hooks Specification 1.0, http://cds-hooks.org/specification/1.0/
- Hooks Specification, http://cds-hooks.org/hooks/
- CDS Hooks Examples, http://cds-hooks.org/examples/
- Discussion of CDS Hooks security issues, https://github.com/cds-hooks/docs/labels/security-review
- Historical discussion of the CDS Hooks security approach, https://github.com/cds-hooks/docs/labels/security-review
- Discussion of CDS Security Model, https://github.com/cds-hooks/docs/pull/72
- CDS Hooks Use Cases, https://github.com/cds-hooks/cds-hooks/wiki/Use-Cases

Sources relating to OAuth 2.0 and its associated security risks and remedies:

- The OAuth 2.0 Authorization Framework, RFC 6749, https://tools.ietf.org/html/rfc6749
- The OAuth 2.0 Threat Model and Security Considerations, RFC 6819, https://tools.ietf.org/html/rfc6819
- The OAuth 2.0 Authorization Framework: Bearer token usage, RFC 6750, https://tools.ietf.org/html/rfc6750.
- JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants, RFC 7523, https://tools.ietf.org/html/rfc7523
- Open Web Application Security Project (OWASP), HTML5 Security Cheat Sheet, https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet

The CDS Hooks subject matter experts -- specifically, Kevin Shekleton, Isaac Vetter, and Brett Marquard -- also were significant sources of information regarding CDS Hooks.

2.2 Process

This security risk assessment process included the following activities.

1. Review of available resources, and identification of security risks associated with each interaction defined in the Scope above.
2. Documenting risks.
3. Categorizing severity of risk as high, medium, or low.
4. For each identified risk, assessment of whether and how the CDS Hooks specification has addressed the risk.
5. Recommendation of countermeasures.

6. Iterative review of the draft assessment with the CDS Hooks team.
7. Documenting changes to the Specification 1.0 implemented during the course of the risk assessment.
8. Review of draft Risk Assessment Report with CDS Hooks team; revision as needed.
9. Delivery of final CDS Hooks Risk Assessment Report.

Risk severity levels are defined as given in Table 1:

Risk Level	**Risk Level Definitions**
High	Risk warrants immediate implementation of strong corrective measures.
Medium	Risk warrants corrective actions to be taken within a reasonable period of time.
Low	Risk likelihood is low and/or potential loss may be tolerated. CDS Hooks leadership should determine whether to take corrective actions or to accept risk.

Table 1. Four levels of risk severity.

3 Findings

Specific results of the risk assessment are given in Appendix A. Each row provides:

1. Risk Identifier (R*x*)
2. Risk Description
3. Risk Association (as identified in Figure 1)
4. Risk Level (as defined in Table 1)
5. Recommended countermeasures

A total of 17 individual security and safety risks were identified, and categorized as shown in Table 1, along with the associated exchanges and services. All of the risks identified were remediated or mitigated by changes made to the CDS Hooks specification.

Risk	**EHR>CDS**	**CDS>FHIR**	**CDS>EHR**	**Cards**	**Browser**
The risk that confidential information and privileged authorizations transmitted between an EHR and a CDS Service could be surreptitiously intercepted by an attacker.	✓	✓	✓	✓	✓

Risk	EHR>CDS	CDS>FHIR	CDS>EHR	Cards	Browser
The risk that an attacker masquerading as a legitimate CDS Service could receive confidential information or privileged authorization from an EHR (via prefetch or FHIR retrieval), or could provide to an EHR decision support recommendations that could be harmful to the patient.	✓	✓	✓	✓	
The risk that an attacker masquerading as a legitimate service-subscribing EHR (i.e., man-in-the-middle) could intercept patient data and decisions exchanged between the two parties, exposing sensitive patient data and possibly altering clinical data or returned Cards.	✓				
The risk that the FHIR resources provided to the CDS Service could exceed the “minimum necessary.”	✓	✓			
The risk that a CDS Service could embed dangerous suggestions or links to dangerous apps in Cards returned to an EHR.				✓	
The risk that a CDS Hooks browser-based deployment could be victimized by a Cross-Origin Resource Sharing (CORS) attack.					✓
The risk that a CDS Service could return a decision based on outdated patient data, resulting in a safety risk to the patient.	✓	✓			

Risk	EHR>CDS	CDS>FHIR	CDS>EHR	Cards	Browser
Implementation risks resulting from ambiguities inherent in the CDS Hooks specification.	✓	✓	✓	✓	✓

4 Modifications to CDS Hooks Specification V1.0

A total of 21 GitHub Pull Requests (PRs) were submitted, approved, and merged as part of this Risk Assessment. Appendix B contains a log of the changes made to CDS Hooks Specification 1.0. The columns in the log show:

1. GitHub Pull Request Number
2. Date Submitted
3. Title
4. Brief Description
5. Risk Identifier (ref Appendix A)

This section consolidates and summarizes these changes.

4.1 Reducing Specification Ambiguity and Optionality

Ref: Risks R6 and R14

A section titled “Conformance Language” was added, clarifying that the key words defined by RFC 2119, “Key Words for Use in RFCs to Indicate Requirement Levels,” are used in the CDS Hooks specification. A “Priority” column was added to all field-definitions tables used in the CDS Hooks API, along with the priority (e.g., REQUIRED, RECOMMENDED, OPTIONAL) for each field. Also, a “Limitations” section was added to clarify the scope of the CDS Hooks specification.

In some cases, the CDS Hooks community seemed to have reached consensus on requirements that were not clearly stated as such in the specification. For example, CDS Hooks requires that all exchanges among EHR entities and CDS Services must be secured using the Transport Layer Security protocol (RFC 5246), but the specification had not articulated this requirement. Similarly, the specification had not captured the requirement that GitHub Markdown without HTML be used in CDS Hooks Cards as a countermeasure against Cards returning text markdown with spurious HTML, nor the requirement that each CDS Service MUST expose a stable end point for discovery.

Much of the security assurance provided by CDS Hooks is dependent upon negotiations that occur out-of-band and that were not clearly described in the specification. For example, through out-of-band negotiations with the CDS Service provider, the EHR vendor/provider agree upon whether the EHR will prefetch FHIR resources and transmit them in the CDS Service call, and if so, what resources will be prefetched. Similarly, through these negotiations, the EHR vendor/provider and the CDS Service provider agree upon whether the EHR will pre-fetch an access token on behalf of the CDS Service and provide it in the CDS Service call. As these negotiations are critical to managing security risks associated with the CDS Hooks API, they were added to the specification.

The CDS Service Response table was challenging to follow because the nesting of field tables was unclear. Section and subsection headers and explanatory text were added, and some content was moved, to help clarify the contents of Cards returned by CDS Services.

In one case, the fields shown in an example did not coincide with those shown in the corresponding field-definitions table. Also, due to a publishing tool used earlier, all of the examples appeared before the tables defining the fields illustrated in the examples (a simple fix).

4.2 Providing FHIR Resources to a CDS Service

Ref: Risks R3, R5, R11, R13, R15

From a security perspective, the preferred approach for providing FHIR resources to a CDS Service would be to have an EHR launch a CDS Service passing only context data. The registered CDS Service would then request authorization directly from the EHR's authorization server, which would mediate the request and if approved, return an access token that would enable the Service to retrieve the necessary resources directly from the EHR's FHIR server. However, because CDS Services must respond very quickly, the CDS Hooks specification provides two performance enhancements that allow a CDS Service to request and obtain FHIR resources more efficiently -- having the EHR prefetch the necessary resources and pass them in the CDS Service invocation, and having the EHR obtain an access token authorized for use by the CDS Service to retrieve FHIR resources.

In the pre-existing specification, data "prefetching" was discussed in two separate sections and was addressed independently from the EHR's obtaining and passing an access token for the Service's use. However, both prefetching of FHIR resources, and preauthorization of an access token, are approaches an EHR can optionally use to provide FHIR resources to a CDS Service. Both approaches are designed to enhance CDS Hooks performance by avoiding forcing the CDS Service to request authorization directly from the EHR's authorization server each time a resource is required. And both approaches are associated with attendant security risks, including potential disclosure of sensitive clinical data and risks associated with the use of bearer access tokens. (See *The OAuth 2.0 Authorization Framework* (RFC 6749) and *The*

OAuth 2.0 Authorization Framework: Bearer Token Usage (RFC 6750) for a discussion of these risks.)

Regardless of the approach used, the EHR must assure that the clinical data provided to the CDS Service are limited to the data to which the current user has access, and that the Service is given the most current data available, as decisions based on stale data pose a safety risk to the patient. To assure that all of these considerations are addressed, the terms associated with the chosen approach need to be negotiated out-of-band between the EHR vendor/provider and the CDS Service, consistent with the EHR vendor/provider's performance requirements and tolerance for security risk.

To help clarify these points, a new section entitled "Providing FHIR Resources to a CDS Service" was added to the specification. The new section includes a discussion of both resource prefetching and proxy-authorization of a bearer access token as efficient means of providing data to the CDS Service. The need for pre-negotiation of details regarding how these services will be used, and the architectural dependence of their implementation, are also addressed in this new section.

The pre-existing Prefetch Template was pulled into the new section, and a discussion of FHIR resource access was added. Although the CDS Hooks community recognized the need for the bearer access token to be issued specifically for use by the CDS Service, how this client association was established was not clear. The new section explicitly states that the access token is associated with the specific CDS Service, user, and context of the invocation, and that the data to which the CDS Service is given access MUST BE limited to the same restrictions and authorizations afforded the current user. Requirements for a high-entropy token, a short expiry time, and prohibitions against caching were also included.

4.3 Security and Safety Section

Ref: Risks R1, R2, R4, R7, R8, R9, R10, and R12

Extensively revised the pre-existing "Security" section, beginning with an articulation of the security and safety risks associated with CDS Hooks, and the need for each individual EHR vendor/provider to perform a due diligence on each CDS Service provider whose service they are contemplating using, and to develop and maintaining a "white list" of services they deem trustworthy. The section discusses the importance of the negotiation process between the EHR vendor/provider and the CDS Service prior to signing a service agreement, and the need for the CDS Service to be pre-registered with the EHR's authorization server.

Fields added to the JWT used to authenticate the EHR to the CDS Service were: "iss" for the issuer of the JWT, "sub" for the EHR being authenticated, and "kid" for the identifier of the key pair used to sign the JWT. Separating the "issuer" of the JWT from the "subject" allows potential for a third-party issuance, such as the use of an OpenID Connect ID provider. The

requirement for the EHR to use JSON Web Signatures (RFC7515) to digitally sign the JWT was also added.

The pre-existing specification included a section on Cross-Origin Resource Sharing (CORS) that primarily discussed security risks associated with the use of the CDS Hooks Sandbox, a browser-based application that uses CORS. Because the Sandbox is a tool offered for use in testing CDS Services, it is outside the scope of the CDS Hooks API specification.

Most of this content was replaced with a simple clarification that all CDS Services, and browser-based EHRs that use CDS Services, will need to implement CORS, along with a reference to guidelines published by the Open Web Application Security Project (OWASP) regarding secure use of CORS.

Appendix A: CDS Hooks Security Risks

ID	Risk Description	Risk	Risk	Recommended Countermeasures
R1	Cards returning text markdown contain spurious HTML, resulting in cross-site scripting (XSS) attack.	Card Svcs	H	Agree with current approach of using Github-flavored Markdown without HTML. Suggest adding to spec that the use of Gibhub-flavored Markdown without HTML is REQUIRED for all CDS Hooks Cards.
R2	Malicious code embedded in app linked to suggestion card or app link card results in data confidentiality or integrity breach, or interruption in availability of EHR services.	Card Svcs	H	Incorporate basic guidance stating that every individual health sytem should determine the safety and integrity of CDS Services it uses, based on the organization's risk management strategy. Recognize that EHR vendors may make recommendations. Provider should maintain a "white list" (and/or "black list") of CDS Services they have vetted. May also maintain a "white list"/"black list" of links they will display. Any restrictions will be enforced by the EHR authorization server.
R3	CDS Service makes clinical decision based on "prefetched" data, or data retrieved from FHIR server, that may have been superceded, resulting in a CDS decision based on expired/stale data. This creates a safety risk to the patient and liability risk for the provider organization.	EHR->CDS CDS->FHIR	L	Recommend identifying this risk in the spec and note the importance of assuring that CDS decisions are based on fresh data, and that prefetched data should be acted upon immediately -- else retrieve new FHIR resources. Suggest that the spec indicate that including "prefetched" data in the service call is RECOMMENDED as a performance enhancement, but is not REQUIRED.
R4	Risk that CDS Service uses unsecured URL for HTTP calls to FHIR Server or redirect URI, exposing sensitive information through URL. (In spec, JSON POST body shows FHIR server URI and redirect URI as unsecured links.)	CDS->FHIR	M	Clearly state in spec that all exchanges between the EHR and the CDS Service, and between the CDS Service and EHR FHIR server MUST be secured using TLS.

ID	Risk Description	Risk	Risk	Recommended Countermeasures
R5	CDS Service call includes an OAuth 2.0 "bearer" token issued to the EHR app, which the EHR app passes on to the CDS Service for use in retrieving FHIR resources from the FHIR Server. Because a bearer token can be used by any "bearer," risk that and intercepted or otherwise captured token could be used by an unintended client. The bearer token can be obtained in a number of ways -- e.g., from open HTTP connection between EHR and CDS Service (http instead of https), inadequate protection of tokens stored by the EHR app, authorization server, or CDS server, or by spoofing the FHIR Server's network address. The attacker then can use the token to access protected resources. In addition, this approach incurs repudiation risk, as any actions taken by the CDS Service can be attributed to the EHR app to whom the bearer token was issued.	EHR->CDS	H	Recommend: 1. Consider requiring the CDS Service to request authorization directly from the EHR authorization server, which issues the token directly to the CDS Service, consistent with the SMART app protocol (http://docs.smarthealthit.org/authorization/), which includes short expiry and a no-caching requirement. 2. If the EHR app obtains the token on behalf of the CDS service, require that the request sent from the EHR app to the authorization server include the registered identity of the CDS service that will be using the app (e.g., "sub" field). Limit scope to that authorized for the current user. Require short expiry, and no caching of tokens by either the EHR app or CDS service. Require that access token transmitted from EHR to CDS Service be digitally signed by the EHR.
R6	Fields included in the example are inconsistent with those specified for the CDS Service call (HTTP Request). Fields missing in the example: fhirAuthorization (i.e., access token), encounter.	EHR->CDS	L	Assure that examples reflect requires specified.
R7	EHR FHIR Server receives bearer token from service masquerading as a known CDS Service. Since "bearer" token is associated only with the EHR to which it was issued, any malicious actions taken by CDS Service cannot be attributed to that service.	CDS->FHIR	L	Recommend: 1. Requiring all authorized CDS Services to pre-registered with the EHR authorization server. 2. Include CDS Service identity in request for bearer token.
R8	Disclosure of sensitive information passed among participating entities.	All	L	Clearly state in spec that all exchanges between the EHR and the CDS Service, and between the CDS Service and EHR FHIR server MUST be secured using TLS.

ID	Risk Description	Risk	Risk	Recommended Countermeasures
R9	JWT token used to authenticate EHR's identity to CDS Service contains neither the identity field (sub) nor an index to the keypair used to digitally sign the token (kid), creating risk that CDS Service will misassociate the JWT.	EHR->CDS	M	Suggest using a JWT authentication token per RFC 7523 (https://tools.ietf.org/html/rfc7523#page-5) wherein the "iss" field provides the URI of the issuer and the "sub" field identifies the client_id by which the CDS Service knows the EHR. Using "iss" to identify issuer enables use of 3rd-party identity provider. In cases where JWT is issued by EHR, "iss" could identity authorization server and "sub" the EHR application. Also, add a "kid" parameter for the key_id of the keypair used to digitally sign the token. References to keys used are communicated in advance, perhaps within the registration process. (See R16)
R10	Client masquerading as CDS Service client, connecting through a secured TLS link, attempts to use CDS services.	EHR->CDS	L	The spec says “At this time, CDS Hooks does not prescribe how the EHR shares its public key or the format of said key used in the JWT signature.” CDS Hooks will need the EHR's public key in order to use the authentication JWT. Note that RFC 7523 (see R16 below) uses the "kid" header value for this purpose, where kid = Key_id of the keypair used to digitally sign this token. Recommendation R16 in its entirety applies here.
R11	Unauthorized exposure and use of the "bearer" access token.	EHR->CDS CDS->FHIR	H	Recommend: * Protect tokens in transit (TLS) and at rest * Assure that access tokens cannot be generated, modified or guessed (high entropy) * EHR and CDS Hooks profile should request minimal scope; authorization server should grant minimal scope * Neither EHR nor CDS service should store bearer tokens in unencrypted cache (no-cache should be specified with returned token)
R12	Browser-based EHRs must implement Cross-Origin Resource Sharing (CORS) in order to call CDS Services, and the called Services must support CORS calls. Also, because the CDS Hooks Sandbox is a browser application, CDS Services must implement CORS to use the Sandbox for testing. Browser-based EHRs are subject to risks associated with CORS implementations, including unauthorized access to resources and injection of malicious code.	Browser	H	CORS is relevant only to exchanges between browser-based EHR implementations and CDS Services. The CDS Hooks Sandbox is a resource made available to CDS Hooks developers, and details regarding its use should be provided outside the CDS Hooks specification. Recommend removing CORS from the CDS Hooks specification, and replacing this content with a reference to considerations when including CORS in the CDS implementation -- e.g., OWASP recommendations at https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet

ID	Risk Description	Risk	Risk	Recommended Countermeasures
R13	With no constraints on the "prefetch" field of the CDS Service description, risks that a CDS Service description may request FHIR data scope far beyond what is required to make the requested decision (e.g., */*.read), or that EHR prefetches and sends more data than necessary. Both cases violate the "minimum necessary" rule and create privacy risk for the patient and compliance risk for the provider.	EHR->CDS CDS->FHIR	M	CDS Hooks service providers will provide clinical services, and as such will be responsible (as HIPAA covered entities or business associates) for enforcing the "minimum necessary" rule. Suggest specifying that "prefetch" field in CDS Service description, prefetched included in service call, and data the CDS Service retrieves from FHIR resource server MUST be the minimum necessary to provide the decision-support service requested.
R14	Vulnerabilities in implementations due to ambiguity in specification.	All	H	Revise specification to clearly indicate actions and fields as REQUIRED, RECOMMENDED, OPTIONAL, or disallowed (MUST NOT, SHOULD NOT, etc.). Clarify that CDS Services MUST expose a stable end point.
R15	Specification does not include requirements or guidelines for APIs that enable CDS Services to request an access token directly from the provider's authorization server -- leaving EHR providers and CDS services open to known vulnerabilities in OAuth 2.0 implementations.	EHR->CDS CDS->FHIR	M	Clarify that CDS Services receive FHIR resources only through prefetching and use of access token passed by EHR.

ID	Risk Description	Risk	Risk	Recommended Countermeasures
R16	The CDS Hooks approach to authenticating the EHR to the CDS Service uses a JWT token that is encrypted by the EHR, but contains no identification of the subject being authenticated (i.e., "sub" parameter). To set up the TLS connection between the EHR and the CDS Service, the EHR will have authenticated the CDS server, but the CDS Service has no way of knowing the identity of the EHR. The JWT needs to contain the identity being authenticated by the digital signature.	EHR->CDS	H	Recommend adopting RFC 7523 (JWT Authentication Profile for OAuth 2.0 Client Authentication) as standard for EHR authentication. The claims required by RFC 7523 are quite similar to those prescribed for CDS Hooks EHR authentication. Conformance with RFC 7523 requires the following changes: * specification of RFC 7523 as the standard for EHR authentication in the CDS Hooks spec * specifying the following parameters as REQUIRED: iss, aud, exp * adding "sub" as a REQUIRED parameter idenfiying the EHR client_id as the subject of the JWT * REQUIRING that the JWT be digitally signed using JSON Web Signatures (RFC7515), with the keypair identifier specified using the "kid" parameter * REQUIRING that the CDS service MUST reject a JWT that is not valid in all respects Note that the possibility that a third-party might serve as the authenticator (e.g., OpenID Connect service provider, as mentioned in PR#72) reinforces the need to include a “sub” field to identify the EHR (client_id), as the iss field could be a 3rd-party issuer (or the EHR, if self-issued). If issued by 3rd party, should still be signed by EHR, with "kid" field identifying the key-pair used for the signature.
R17	Token redirect: CDS Service uses bearer token provided by EHR app to obtain FHIR data from a resource server not intended or authorized for use by CDS Services.	CDS->FHIR	M	Add the "aud" (audience) parameter to the specification of the "fhirAuthorization" field so that the token can be presented only to the FHIR resource server specified. Then, upon receipt of an access token, the FHIR server needs to check to assure that the access token it has received is intended for its consumption.

Appendix B: Log of Changes Made to CDS Hooks Specification 1.0

PR#	Date	Title	Description	Risk ID
126	12/19/17	Indicate the required fields in a Discovery CDS Service Definition	Tightened up table showing fields in a service description such that each field has an associated "priority" of REQUIRED, RECOMMENDED, or OPTIONAL (not used in this example). This change illustrates the recommendation that the 1.0 spec needs to be specified more explicitly. In addition, it carries out the recommendation to make the Prefetch field OPTIONAL rather than required, so that each provider can decide whether to prefetch or allow the CDS service to fetch its own data as needed.	R14, R3
127	12/21/17	Update	CDS Services SHALL expose "stable" endpoint	R14
129	12/21/17	Service Registration	New content re service registration and "white listing"/"black listing." Clarify that URLS need to have been deemed safe.	R2
130	12/21/17	Add documentation that all communications occurs over TLS	Added TLS requirement.	R4, R8, R11
131	12/21/17	Card Attributes	Added priority field to table. Added GitHub Markdown without HTML requirement.	R1
132	12/21/17	Prefetch Clarifications	Clarification of issues discussed w.r.t. prefetch, its need to be pre-negotiated, and the architectural dependence of its implementation.	R3
135	1/4/18	Minimum necessary in CDS description	Added clarification that the data elements a CDS service requests to be prefetched needs to be the "minimum necessary." Added priorities to table.	R13
136	1/4/18	Performance Enhancements	Clearly separated the two "prefetch" sections, with the first discussing both performance enhancement options for providing data (i.e., prefetch and passing bearer token), and the 2nd a technical specification of the "prefetch template." Renamed the 1st "prefetch" section "Providing FHIR Resources to the CDS Service" and the 2nd "Prefetch Template." Moved "discussion" content out of "Template" section and into "Providing FHIR..." section. Also, added need for "fresh" data w.r.t. safety risk.	R3, R15

PR#	Date	Title	Description	Risk ID
137	1/5/18	FHIR Resource Access	Incorporates all of the concepts discussed w.r.t. enabling an EHR to obtain a bearer token on behalf of a CDS service, and passing it on to that service in the service request. Moved all of the pre-existing discussion re SMART into introductory section so that the specification sections could be purely specification. Added requirement for no-cache. RFC7521 defines the "subject" parameter as "an authorized accessor for which the access token is being requested," so incorporated as registered identifier of the CDS Service that will be using the token. [Detail regarding parameters used to obtain the access token were subsequently eliminated by PR #167.]	R5, R7
138	1/5/18	Calling a CDS Service Edits	Modified example to align with parameters table by adding "fhirAuthorization" and "encounter" fields." Reworded description of "fhirAuthorization" parameter.	R6
139	1/11/18	New Security and Safety Content	New and revised content for Security and Safety section. Moved example to follow parameters chart.	R2, R3, R4, R7, R8, R9, R10
140	1/11/18	Cross-Origin Resource Sharing	Replaced most of this content with simple statement regarding CORS and a reference to the OWASP guidelines. Clarified that all CDS services and browser-based EHRs will need to implement CORS.	R12
141	1/17/18	RFC2119	Added explanation that RFC2119 standards terminology is used.	R14
142	1/18/18	Limitations	Added "Limitations" section to "Overview."	R14
143	1/18/18	CDS Service Response Changes	Moved the example to follow the field specifications. Added "Priority" to all tables (except for the Card Attributes because Priorities were added by PR #131). Added sub-sections to show nesting of attributes. Integrated "No Decision Support" content into "Card Array" section. Integrated "Analytics" content into "Suggestion" section.	R14
146	1/25/18	Discovery Example	Moved JSON to follow specification.	R14

PR#	Date	Title	Description	Risk ID
147	1/25/18	Providing FHIR Resources convergence	Pulled "Prefetch Template" and "FHIR Resource Access" into "Providing FHIR Resources to a CDS Service" section, as intended by PRs #132, #136, and #145.	R3
148	1/25/18	Calling a CDS Service Mods	1) Moved the example JSON to follow the specification 2) Added priorities to the HTTP request fields table. NOTE: We discussed the fact that aud should not be included in the fhirAuthorization structure because fhirServer was specified outside the fhirAuthorization structure. However, a dependency exists between the two: if fhirAuthorization is included, a fhirServer MUST be specified. Made them both OPTIONAL, and noted that if fhirAuthorization is included, fhirServer is REQUIRED. The suggestion to move the fhirServer parameter to inside the fhirAuthorization structure so that fhirAuthorization could be OPTIONAL, with fhirServer REQUIRED (as a parameter of fhirAuthorization) was presented to the CDS Hooks community. Use cases in which fhirAuthorization was not provided, but fhirServer was still required, were identified. So the decision was made to leave fhirServer as an independent OPTIONAL parameter that is REQUIRED if fhirAuthorization is provided.	R14
149	1/25/18	Card Array Attributes	Added Priorities to table. Also added "without HTML" to ref to Github-flavored markdown, per our discussion.	R1, R14
150	1/25/18	Recovered content	Recovered content formerly merged as PR #129 and subsequently overwritten by another change.	R2
160	1/29/18	"Context" specification reference	Because "context" is included in the HTTP call to invoke a CDS Service, developers will need to know its contents. Added reference to the Hooks specification, where "context" is defined.	R14
167	2/15/18	Refine authorization details around how the EHR obtains an access token on behalf of the CDS service	Removed mention of the specifics of how an EHR is to obtain an access token on behalf of the CDS Service. Instead, the documentation just lays out what the access code needs to honor. Also required that the scope of access given to the CDS Service be limited to the access authorized for the current user.	R5