**ONC Watch For Digital Health App Developers**

Author: Jill DeGraff, Managing Member, Aperture Law Group PLLC

First Published March 8, 2019

On February 11, 2019, the Office of the National Coordinator for Health Information Technology (ONC) released its [Notice of Proposed Rulemaking](https://www.healthit.gov/topic/laws-regulation-and-policy/notice-proposed-rulemaking-improve-interoperability-health) for implementing provisions of the 21st Century Cures Act. The proposed rule would promote interoperability of electronic health information, increase patient access to their health data, alleviate administrative burdens of electronic health recordkeeping for health care providers and counteract anticompetitive practices that developed as electronic health record technologies were adopted, like information blocking.

This ONC Watch is written for digital health app developers.

[**What is ONC’s role in promoting interoperability and patient access to their information?**](#ONCRole)

[**How does the ONC perform its role as a convener?**](#ONCPerformance)

[**Does the ONC regulate digital health app developers?**](#ONCRelationship)

[**Why should app developers care about the ONC and its Proposed Rule?**](#WhyCare)

[**Do I calibrate my roadmap to the ONC’s timeline?**](#WhatChange)

[**What are some key take-aways that I can take from ONC’s proposed rules for expanding interoperability in healthcare?**](#TakeAways)

# What Is ONC’s Role in Promoting Interoperability and Patient Access to their Information?

The ONC serves as a convener for the advancement of health information technologies (HIT) in health care delivery.

[back](#ONCRole)

# How Does the ONC Perform Its Role as a Convener?

The ONC engages in iterative, consultative rulemaking with stakeholders from the public and private sector, including sister agencies, healthcare providers, technology developers and patient advocates. The ONC works jointly with stakeholders to arrive at consensus standards, and timetables for implementing these standards in an ordered, step-wise progression. Accordingly, proposed and final rules reflect industry-wide consensus, and provide a transparent baseline of market guidance. The ONC’s primary mechanism for implementing consensus standards are the criteria for certification of electronic health record technologies (CEHRT). The current criteria are reflected in the year 2015 edition. Proposed regulations reflect changes to the 2015 Certification Criteria.

[back](#ONCRole)

# Does the ONC Regulate Digital Health App Developers?

No. The ONC’s regulatory or enforcement authority is defined by the Certification Criteria that it establishes for CEHRTs. Even so, the ONC seeks alignment with the wider developer community, viewing the community as a necessary innovation resource, particularly as modern computing methods mature and evolve.

[back](#ONCRole)

# Why Should Digital Health App Developers Care About the ONC and Its Proposed Rule?

Aspirationally, the ONC’s vision is for electronic health information to be liberated for use in the broader app economy, so that patients can achieve the same benefits they receive from apps that connect them to their bank balances, airline ticket information, favorite sports teams’ scores, local weather and traffic data. Getting there takes incremental steps in building the standards-based interoperability infrastructure and preparing the healthcare ecosystem for scalable interoperability around a sequence of defined patient datasets and elements. In a later post, I’ll talk more about the first types of data sets and data elements that app developers can expect to come down the emerging electronic health interoperability highway.

[back](#ONCRole)

# Do I Calibrate My Roadmap to the ONC’s Timeline?

It will take years for ONC rules, once finalized, to be fully implemented by CEHRT vendors, and then for healthcare providers to implement those technologies. On the one hand, digital health app developers need to check their expectations about the timing for realizing any kind of scale with services that rely on the types of data that ONC is working to liberate from EHRs. On the other hand, innovation is already happening, evidenced by a wide number of industry- and developer-supported interoperability ecosystems. In that respect, the proposed rules are like a snapshot in time, perhaps reflecting a bit of “yesterday’s news”. But they can also help orient app developers as think strategically as they define their respective paths to market.

# What Are Some Key Take-Aways That I Can Take from ONC’s Proposed Rules for Expanding Interoperability in Healthcare?

Here are six take-aways from the ONC’s proposed rule for digital health app developers.

## FHIR is considered the *de facto* API Standard for Liberating PHI from EHRs

“[W]hen we look at the app economy and the clear trends in modern computing, one API approach seems to clearly emerge – Health Level Seven’s (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards.” That’s how the National Coordinator for Health Information Technology, Don Rucker, put it in a [blog accompanying the proposed rulemaking](https://www.healthit.gov/buzz-blog/interoperability/oncs-proposed-rule-will-connect-people-to-their-care).

Under Section 170.315(g)(10) of the proposed rule, HIT vendors will be required to certify that their technologies include a “standardized API for patient and population services”. The technical outcomes and conditions that must be supported in these APIs are listed in Section 170.315(g)(10), starting on page 639 of the Proposed Rule (based on the link provided at the top of this blog). These outcomes and conditions include such things as data response times, search support, app registration through the CEHRT’s authorization server, establishing secure and trusted connections, establishing authentication and app authorization processes, and providing documentation and consent management capabilities that meet minimum standards enumerated in the proposed rule.

FHIR Release 2 is proposed as the new API baseline standard, as stated in Section 170.215(a)(1)(starting on page 625). However, the ONC observes that the industry will be implementing Release 4 in parallel with the proposed rulemaking. For that reason, it requests comment on whether to skip wide-scale production deployment of FHIR Release 3, which is not yet widely deployed in the industry, and define a glidepath for FHIR Release 4 into the certification criteria.

The proposed rule also defines a minimum set of FHIR implementation specifications, referred to as a base set of FHIR resources called the API Resource Collection in Health or “[the ARCH](https://www.healthit.gov/ARCH)”. See Section 170.215(a)(2)(starting on page 625). The purpose of the ARCH is to further constrain the resources needed to support the first data sets and data elements that ONC has proposed to for inclusion in the U.S. Core Data for Interoperability standard of the 2015 Certification Criteria. (To be discussed further in a later blog).

Assuming the proposed rule is enacted, APIs would be oriented around requirements that facilitate interoperability for services (1) for which a single patient’s data is the focus and (2) for which multiple patients’ data are the focus.

For a single patient’s data, CEHRTs would have to support the timely creation of export file(s) with all of a single patient’s electronic health information that the system produces and electronically manages. This functionality would have to be supported without the developer’s intervention and at any time a user chooses. The export file would have to be electronic and in a computable format (not a .pdf, for example). The export file’s format, including structure and syntax, would need to be included with the file.

For a database export, CEHRTs would have to support the creation of all electronic health information that the system produces and electronically manages. The export file would have to be electronic and in a computable format (not a .pdf, for example). All documentation for the export format would need to be made available via a publicly accessible link.

## The ONC Adopts Standards and Implementation Specifications for Persistent Authentication, App Authorization and Patient Access

For user authentication, ONC proposes to adopt the [OpenID](http://openid.net/) Connect Core 1.0 incorporating errata set 1 standard, as it complements FHIR’s SMART Application Launch Framework Implementation Guide Release 1.0.0. In commentary, ONC explains that OpenID is typically paired with OAuth2 and focuses on user authentication. The proposal also recommends adoption of SMART, with additional details for the use of specific resources. Examples include the use of “refresh tokens” for a minimum life of 3 months to strike a balance between security and persistent patient access to their applications.

## ONC Recommends Encryption of Authentication Credentials, To Complement Existing Requirements for Encrypting Patient Data

Current certification requirements provide for all patient information saved on end-user devices to be encrypted, but does not affirmatively require authentication credentials to be protected, which introduces a security vulnerability. To address this gap, the ONC proposes a new attestation in which HIT vendors would attest whether or not their technologies encrypt all authentication credentials. See Section 170.315(d)(12), starting on page 634). ONC chooses not to affirmatively require encryption of authentication credentials in all cases. However, if HIT vendors affirmatively attest to this criterion, the proposed attestation would tie to FIPS 140-2 cryptography requirements, which the ONC commentary regards as the “seminal, comprehensive and most appropriate standard”.

Practice tip: Digital health app developers should strongly consider implementing FIPS 140-2 cryptography in their applications, if they are not doing so already, and remember to encrypt authentication credentials in their own applications.

## The ONC Encourages the Use of Multi-Factor Authentication in any Service that Gives Access to Any Personal Data

Under the proposed rule, HIT vendors would also be required to attest whether or not their technologies leverage the multi-factor authentication (MFA) capabilities of end-user devices. See Section 170.315(d)(13), staring at page 634. The attestation would also address whether their MFA implementation, where applicable, conforms with industry recognized standards like NIST SP 800-63B Digital Authentication or ISO 27001. In commentary accompanying the proposed rule points to the Healthcare Industry Task Force on Cybersecurity’s recommendation that the industry adopt NIST SP 800-46 guidelines in services where any personal data can be remotely accessed.

## More Granular Segmentation of Security Labels to Manage Privacy and Consent Settings Within Summary Care Records (C-CDAs)

One of the current criteria to which CEHRT vendors must certify concerns “data segmentation for privacy” (DS4P) for summary care records (C-CDAs). This means that the CEHRT supports the use of security labels at the document-level based on the HL7 Healthcare Classification (HCS) standard. These security labels ensure that privacy policies established at a record’s source will be understood and enforced by electronic recipients. In its commentary, ONC observed that document-level security levels are not sufficient for privacy and consent management, observing that healthcare providers still resort to manual redaction of sections within documents to comply with applicable state and federal privacy laws. For example, manual redaction may be indicated for a legitimate request for a document a security label on a C-CDA that includes information about a patient’s substance use disorders (subject to the protection of 42 CFR Part 2) would restrict access to the entire document.

Under the proposed rule, ONC introduces a new D24P certification criterion that would support security labels in C-CDAs at the document, section and entry level. ONC also directs developers and organizations to a number of resources to help with implementing DS4P criteria, including the [HHS Security Risk Assessment Tool](http://www.healthit.gov/providers-professionals/security-risk-assessment), the [Guide to Privacy and Security of Electronic Health Information](http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf) and the HHS Office of Civil Rights’ [security risk analysis guidance](https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html).

## Leveraging FHIR Infrastructure To Support Granular Segmentation of Security Labels to Manage Privacy and Consent in FHIR APIs

In commentary to the proposed rule, the ONC observes that the FHIR API infrastructure can be leveraged to share segmented data in a secure and scalable manner, but an industry standard for segmenting and applying security labels on exchanged data has not emerged. Consequently, the ONC recommends that HIT vendors work start with an open source application for data segmentation and consent management that ONC created with the Substance Abuse and Mental Health Services Administration (SAMHSA), called Consent2Share. The aim of Consent2Share is to engage the developer community in efforts to expand support of data segmentation for health care providers engaged in complex use cases, including thosed involved in pediatric care, behavioral health care, HIV/AIDS, alcohol, tobacco, sexuality and reproductive health, and opioid use disorder. As DS4P matures, opportunities for digital health app developers to leverage electronic health information should emerge.

A draft Consent2Share Consent Implementation guide titled “Consent2Share FHIR Profile Design.docx” can be accessed through the Community-Based Care and Privacy (CBCP) HL7 workgroup, within the Package Name titled “BHITS\_FHIR\_Consent\_IG,” at <https://gforge.hl7.org/gf/project/cbcc/frs/>.

[back](#ONCRole)