White Paper – November 2021

IDENTITY, INTEROPERABILITY, PATIENT ACCESS, and the 21st CENTURY CURES ACT:

A Health-ISAC Guide for CISOs

H-ISAC™
HEALTH - ISAC

www.h-isac.org

SCOPE STATEMENT

IDENTITY AND INTEROPERABILITY

An identity-centric approach to enabling secure and easy access to patient data

The modernization of health care over the past decade has been pushed along by the digitization of health information and records into Electronic Health Record ("EHR") systems and Electronic Health Information ("EHI"). While this digitization has been transformational, the full value of digital health care cannot be unleashed without making these records interoperable and easily shareable – enabling patients to have greater access to their own health information and where it flows to. In the United States for example, new federal regulations tied to the implementation of the 21st Century Cures Act now require firms across the health market to enable interoperability of health data though the creation of new APIs designed to facilitate information sharing.

These new interoperability mandates pose significant challenges, not the least of which is ensuring that new systems deployed to enable information sharing do not create new security concerns. Digital identity is front and center in these new interoperability architectures, given the importance of ensuring that only the right people can access sensitive EHI.

This paper – the fourth installment in Health-ISAC's ongoing series focused on helping CISOs implement an identity-centric approach to cybersecurity[1] – will help CISOs understand how an identity-centric approach to securing and enabling access to EHI will allow health organizations to minimize risks involved in complying with the 21st Century Cures Act. While this paper focuses on the new U.S. regulations, the concepts addressed in it apply to any health organization looking to enable broader access to and exchange of EHI. Health-ISAC may look to address a more comprehensive global view of laws, rules and regulations in a future paper.

KEY TAKEAWAYS

1. While APIs are the "door" to enabling interoperability of EHI between health organizations, strong identity solutions are the "key" that keeps EHI secure.
2. Looking beyond compliance and security, healthcare organizations have an opportunity as they deploy more robust identity solutions to modernize the way they deliver healthcare, enabling new innovation that can improve patient experiences. One way of accomplishing this may be through issuing a high assurance digital credential to patients, or partnering with an organization that does.
3. Additional government requirements for high assurance identity vetting and authentication in health care may be coming; prudent planning now can help future proof your organization to address new requirements down the road.

1. Health-ISAC's first paper, Identity for the CISO Not Yet Paying Attention to Identity, explained why identity matters. We followed that with An H-ISAC Framework for CISOs to Manage Identity, outlining how CISOs can implement a comprehensive approach to identity-centric security that will protect against modern attacks and support key business drivers. And our third paper was All About Authentication.

INTRODUCTION

The 21st Century Cures Act, meant to improve the discovery, development, and delivery of new treatments and cures, passed both houses of the U.S. Congress with strong bipartisan support and was signed into law in December of 2016. A key problem the Act was designed to address was the need to catalyze a shift from unconnected siloes of health data that stymied information sharing toward an ecosystem that enabled easy, interoperable, and secure exchanges of EHI. In essence, the law states that patients should have more control of – and easier access to – their own health data, allowing them to access and share it wherever, whenever, and with whomever they want.

To accomplish this, the Act set about standardizing the way "covered data" is to be exchanged so as to make health data accessible, while also removing barriers that prevent the flow of such data – all while keeping the data secure and private, in a way that is efficient and cost effective.

INTEROPERABILITY BASICS

Who does Interoperability apply to?

- Health providers and health IT vendors – who must follow rules from the Office of the National Coordinator (ONC) for Health IT in the Department of Health and Human Services (HHS) enabling patients to access EHI and download or transmit those records via an API. Here, the focus is largely on a new Fast Healthcare Interoperability Resources (FHIR) "Patient Access API" developed by the non-profit standards group Health Level 7 (HL7) that allows patients to easily access data through a third party app of their choice.

Interoperability defined

The 21st Century Cures Act defines interoperability as:

"Health information technology that enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user, allowing for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law"[2]

- Insurers – who must follow rules from the Center for Medicare and Medicaid Services (CMS) to implement APIs that enable "health plan to health plan" data exchange, such as letting patients access and transfer certain claims and clinical data, as well as pending and active prior authorization decisions.[3] Here, the focus is largely on new "Payer to Payer Data Exchange APIs" and "Provider Directory APIs."

The regulations focus heavily on the concept of "Information Blocking" – defined as "business, technical, and organizational practices that prevent or materially discourage the access, exchange or use of EHI when an Actor knows, or should know, that these practices are likely to interfere with access, exchange, or use of EHI."

2. 45 C.F.R. § 170.404(a)(1).
3. Note that the CMS regulations only apply to government-funded health plans, but in practice, many major insurers are implementing this functionality for all their customers.

In simple terms: if a patient asks any of these organizations to share their health data, that organization must enable it. Denial of a request to share EHI is considered "information blocking," and may result in fines and penalties.

What might "interoperability" look like in practice?

Let's translate that block of 21st Century Cures Act text into a real-world example of interoperability. As the 21st Century Cures Act envisions it, an individual, Rebecca, accesses a single secure application on her smartphone and is instantly connected with healthcare providers, pharmacies, insurers, and more. She can quickly, easily, and securely navigate this app to check her latest test results, request prescription refills, and even check in on accumulated fitness data – with secure exchange of her data enabled by APIs. Furthermore, Rebecca isn't limited to healthcare organizations she has an existing relationship with; any new doctors or organizations that Rebecca engages with can immediately be sent any necessary EHI via APIs in a format that is instantly recognizable and useable.

WHY IDENTITY MATTERS TO INTEROPERABILITY

To deliver the scenario described above, each party will need to solve numerous privacy, security, and usability challenges rooted in identity. Most patients will access EHI through an API established by their provider or insurer. But in order to do so, it will be important for that health organization to address several key functions tied to identity:

1. **Authentication and Access:** When "John Smith" asks for his health records to be sent to a new doctor, how does an organization know with certainty it is actually John Smith making the request – and not someone posing as him looking to steal his health data? How is this data securely accessed and transmitted after authentication?

2. **Authorization:** If John Smith only wants to share part of his records, how can he do so in a way that simply and efficiently captures his consent?

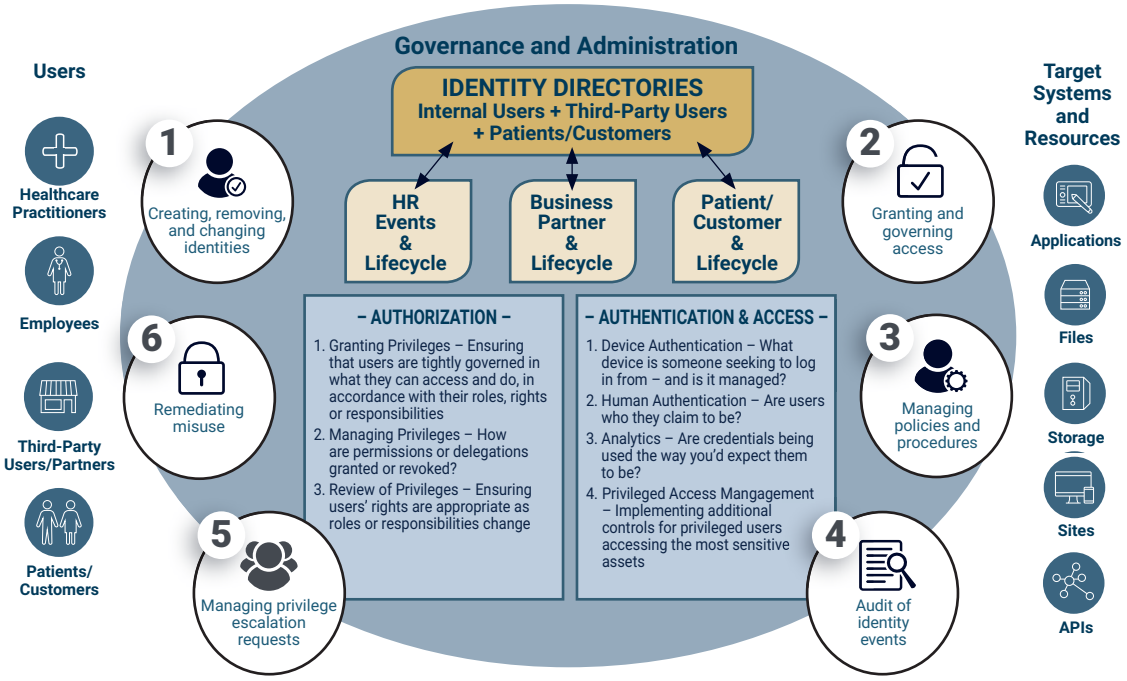
3. **Governance and Administration:** Who creates John Smith's digital identity in the first place? What controls are in place to govern how his credential can be used? What happens if something goes wrong?

4. **Patient Matching:** If the organization has 83 "John Smiths" in its records, how does it know "which John Smith" is making the request? Patient matching errors have led to medical errors for years now, and the potential for errors is now exacerbated as new channels are created for EHI to be shared.

These functions are all covered in the Health-ISAC Identity Framework depicted on the next page. As the Framework details, patients are one of four primary types of users of a health organization's Identity and Access Management (IAM) system.

While the types of access and services patients may need has traditionally varied significantly from what a health care practitioner might require, those lines are starting to blur with the new regulations, given that a patient is now able to request digital access to health data that in many cases was previously only readily available to their provider.

An H-ISAC Framework for Managing Identity



Beyond the Framework, there are other security issues related to identity that are important to solve when it comes to interoperability, including:

- Delegation: How can John Smith access and authorize use of EHI on behalf of someone he cares for, such as a child or an elderly relative? How can he choose to delegate those privileges to someone who cares for him? And how can he choose how long those delegated privileges should last?
- API Level Security: Given that FHIR APIs will be publicly available, how can an organization implement a dynamic approach to secure them after the authorization to use is granted?

The most effective way of mitigating the risk that these issues pose to organizations is through the implementation of a modern, robust, and secure identity infrastructure that can securely authenticate and authorize users and incoming requests, enforce the appropriate consent requests, and tightly govern the use of identities. By design, this is exactly what the Health-ISAC framework is meant to achieve.

Is MFA Required?

While the new ONC and CMS rules do not explicitly mandate multi-factor authentication (MFA), the government guidance points strongly to MFA.

- The ONC rules require Health IT developers and EHR vendors to tell the Department of Health and Human Services (HHS) whether they support MFA and for what use cases. If they do not support MFA, they should "explain why the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry recognized standards."[4]
- The CMS rules note ***"Multifactor authentication represents a best practice for privacy and security in health care settings, and we note that an important benefit of the OAuth 2.0 standard HHS is finalizing is that it provides robust support for multifactor authentication. By requiring that payers subject to our Patient Access API requirement use an API that is conformant with 45 CFR 170.215 (the ONC rules for EHRs), where HHS has finalized the SMART IG, we are supporting the use of multifactor authentication."***

Between this new guidance and the fact that the HHS Office for Civil Rights (OCR) has previously fined health organizations for HIPAA violations tied to inadequate authentication, there are notable risks to health organizations that choose not to use MFA. Health-ISAC detailed how health organizations can best approach implementation of MFA in our last Health-ISAC Identity Series white paper, *"All About Authentication"* – including the importance of adopting phishing-resistant authentication that can block commonly-used attacks to steal one-time passcodes.[5]

But wait – there's more! (Pending ONC Guidance & High Assurance Credentials)

While most health organizations are focused today on the API requirements, draft guidance from ONC would create additional government requirements for high assurance identity vetting and authentication. The draft Trusted Exchange Framework and Common Agreement (TEFCA) is focused on enabling more secure exchange of EHI across health information networks (HINs).

Identity and security play a prominent role in TEFCA's requirements which specifically invoke the Digital Identity Guidelines (SP 800-63-3) published by the National Institute of Standards and Technology (NIST).[6]

Per the latest draft, TEFCA would require that credentials being issued to enable a patient to access their medical information be identity proofed to a minimum of Identity Assurance Level 2 (IAL2) as defined by NIST.[7] And it would require that not just patients but other individuals be authenticated at a minimum of Authenticator Assurance Level 2 (AAL2), as defined by NIST. It would also require participants to support federation at what NIST defines as Federation Assurance Level 2 (FAL2).

Note that TEFCA is a voluntary framework, but as a government-published guideline, it is likely to be highly influential once finalized. This is another reason that health CISOs should be planning for ways to issue high assurance credentials to patients.

4. See https://www.healthit.gov/test-method/multi-factor-authentication and § 170.315 (d)(13) Multi-factor authentication.
5. https://h-isac.org/authentication-a-health-isac-guide-for-cisos/
6. https://csrc.nist.gov/publications/detail/sp/800-63/3/final
7. Section 6.2.4, 7.9 and 8.9 of https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf. Note that ONC has indicated final TEFCA guidance is expected to be published in early 2022.

HOW CISOS SHOULD LOOK TO IMPLEMENT AN IDENTITY-CENTRIC APPROACH TO INTEROPERABILITY

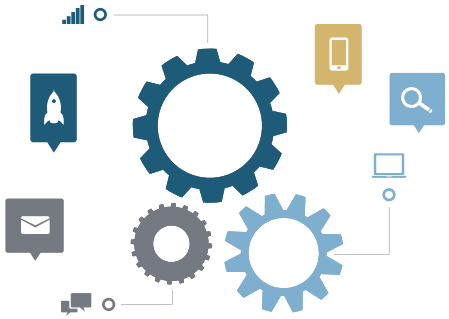
Now that we've established what interoperability is, the reason why healthcare organizations need to adopt it, and how identity ties interoperability into the Health-ISAC's framework, let's breakdown how to go about implementing it.

Compliance

As we've noted, compliance with the requirements of the 21st Century Cures Act is mandatory, and the pending guidance under TEFCA is both unfinalized and optional. As organizations look to become compliant with the Cures Act they will be well-served to not take an approach that fulfills the bare minimum needed to achieve compliance.

A minimalist approach not only represents a lost opportunity to make the most of the investment in time and resources that will be required to carry out this update, but it is also likely to result in a suboptimal implementation that creates needless friction for patients and may introduce new security risks. Furthermore, while the exact nature of the next round of guidance, as illustrated by initiatives like TEFCA, is not completely clear, it is to be expected that it will go above and beyond the Cures Act.

As painful as a single round of significant investment to achieve Cures Act compliance may be, embracing a serious overhaul with implementation rooted in secure identity infrastructure now could save you from having to go through this process twice. More future-ready infrastructure will deliver improved cybersecurity performance and patient interaction.



Implementation

Because the FHIR and SMART standards are ultimately rooted in OAuth and OpenID Connect, insurers, providers, and other health stakeholders will likely find that federation of their identity infrastructure with other healthcare applications is the best option to attaining secure interoperability.

In this instance, identity is what will enable healthcare organizations to go beyond compliance-driven investment and allow them to seek real strategic advantages. This is because robust identity infrastructure can:

- Help organizations launch new health apps and services faster and more securely
- Enable organizations to more easily integrate with other providers and partners
- Streamline work needed to allow for the secure exchange of EHI with other parties – and make it easier to leverage that EHI for analytics that can drive additional insights into care and deliver better health outcomes
- Simplify consent capture and management involving the release of EHI, as well as cutting off access to EHI through an API when consent is revoked
- Empower patients to have more control over their health data and their health care experiences
- Provide improved protection against potential security breaches – especially when phishing resistant MFA is used, per our recommendations in our previous paper *All About Authentication: A Health-ISAC Guide for CISOs*.

CONCLUSION

Identity is a journey. As the healthcare industry focuses on digital adoption, identity will continue to play a foundational role. Whether your implementation of a modern identity system is driven by regulatory and compliance requirements, security and privacy concerns, or a desire to improve customer experience, a well-architected, robust digital identity solution can address all of these drivers.

WHAT'S NEXT?

This paper represents the fourth installment in a Health-ISAC series designed to introduce CISOs to an Identity-centric approach to cybersecurity. The first paper outlined why an Identity-centric approach was needed, the second outlined Health-ISAC's framework for managing identity, and the third examined a key aspect of that framework; authentication. This installment, focused on the patient access aspects of the framework, outlines how the framework and an identity-centric approach is not only directly applicable to meeting new healthcare regulations in the U.S., but how it can provide significant security and business advantages.

More In-depth Analysis

Members should expect subsequent releases to provide in-depth analysis and guidance on many of the issues and technologies introduced in these papers, as well as topical issues related to identity-centric cybersecurity.

Help Shape Future Papers

As we go through this process together, your input will be vital in crafting these follow-on papers. Furthermore, we will provide a means for Health-ISAC members to submit feedback as we consider future papers, so that we may ensure that this series thoroughly examines the aspects that need further clarification or elaboration. Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org.

Helping Organizations of All Sizes and Maturity Levels

Health-ISAC is committed to improving the entire healthcare cybersecurity ecosystem; this series will assist organizations of any size and any cybersecurity maturity in adapting their defense models to address the current threat landscape and become more secure.

KEY TERMS AND ACRONYMS

Electronic Health Information (EHI) – Also known as "electronic Protected Health Information (ePHI)", this term is defined as information that a patient would have the right to request a copy of under the HIPAA Privacy Rule.

Electronic Health Records (EHR) - a digital version of a patient's paper records that provides real-time, patient-centered records, and makes information available instantly and securely to authorized users.

Health Information Exchange (HIE) - An individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI.

Health Information Network (HIN) – A term Interchangeable with HIE (see above definition)

Center for Medicare and Medicaid Services (CMS) – The Federal agency that administers the Medicare program, the federal portion of the Medicaid program and State Children's Health Insurance Program, the Health Insurance Marketplace, and related quality assurance activities. Part of the Department of Health and Human Services (HHS).

Office of the National Coordinator for Health Information and Technology (ONC) – Also part of HHS, ONC is charged with coordination of nationwide efforts to implement and use the most advanced health information technology and enable the electronic exchange of health information.

Office for Civil Rights (OCR) – The part of HHS that enforces HIPAA violations. OCR ensures that individuals receiving services from HHS-conducted or funded programs are not subject to unlawful discrimination, that individuals and entities can exercise their conscience rights and religious freedom, and that individuals can access and trust the privacy and security of their health information.

Fast Healthcare Interoperability Resources (FHIR) - A standard application programming interface (API) used to represent and exchange health information. FHIR is used to help developers build applications and support interoperability in healthcare.

Health Level 7 (HL7) - A non-profit standards development organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information. HL7 houses the FHIR standard.

US Core Data for Interoperability (USCDI) - A standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.

ADDITIONAL RESOURCES

21st Century Cures Act
https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf

CMS Interoperability and Patient Access Final Rule
https://www.federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and

ONC Interoperability and Information Blocking Final Rule
https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification

Trusted Exchange Framework and Common Agreement (TEFCA)
https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org

www.h-isac.org