

---

# The Global Open Health Movement: Empowering People and Saving Lives by Unlocking Data

DRAFT

Lead Editor: Deb Bucci

Status: Working Draft

Date: June 21, 2022

# Contents

[Audience](#)

[Why Open Health?](#)

[Drivers of “Open Health”](#)

[Government Mandates](#)

[Privacy Laws and Data Protections](#)

[“Open Health” Initiatives](#)

[A Global Movement](#)

[Global Health Standards Bodies](#)

[Global “Open Health” Initiative G7 International Patient Summary](#)

[Implementation Considerations](#)

[Identity Profiles](#)

[Consent](#)

[Conformance and Certification](#)

[Why Choose OpenID Foundation Security Profiles](#)

[Overview of Relevant OpenID Foundation Security Profiles](#)

[OpenID Connect](#)

[HEART](#)

[FAPI](#)

[OpenID for Verifiable Credentials](#)

[\[Deb can you insert any health related use cases of note here that would use this use case?\]](#)

[Shared Signals and Events](#)

[Other OpenID Foundation Working & Community Groups](#)

[Other Standards & Tradeoffs](#)

[Recommendations](#)

[Conclusion](#)

[Appendix 1: Country & Regional Standards Participation](#)

[Appendix 2 Health Open Standards In Use today](#)

[Appendix 3 Standards Mapping](#)

[Appendix 4 Verifiable Credential Myths](#)

[Appendix 5 Other OpenID Foundation Efforts](#)

[OpenID Connect for Identity Assurance](#)

[Use of FAPI for Global Assured Identity Network \(GAIN\)](#)

DRAFT

## Audience & Comments

This whitepaper has been written for technologists in the public and private health sectors that are trying to deliver “Open Health,” enabling people to access and share interoperable health data between entities within a health ecosystem, thereby empowering people and improving health outcomes at scale.<sup>1</sup>

As a working draft of this paper, we warmly welcome comments from the global community to ensure we accurately represent the health and identity landscape, and articulate how standards can meet the health community’s goals. **Comments on this paper can be directed to [director@oidf.org](mailto:director@oidf.org).** Our target date for a Final draft of this paper is early September 2022.

## Why Open Health?

How does a health patient’s information move within a doctor’s office? A hospital? A health network? A country? Across countries? If a patient or doctor can’t access the information they need in a timely manner, what is the consequence? If an academic can’t access a full population of patient data, which patients miss a diagnosis?

The core concept of Open Health is to empower a patient to be able to access and share their health data, breaking down the traditional silos of data held in a doctor’s office, hospital or health network. Building effective health IT infrastructure to serve patients is not a new challenge. However, the movement towards giving a “data subject” the right to access and share their data is a newer concept introduced in the EU’s GDPR legislation, in “Consumer Data Right” Legislation in Australia, in the US 21st Century Cures Act and beyond. Open Health policies and regulation is now cascading around the world and driving a wave of compliance obligations on health ecosystems.

Delivering on the potential of these Open Health initiatives, is complicated by six key factors:

- 1) **It’s often extremely sensitive data.** Regulation in most mature markets requires a higher level of privacy and security to access or move health data between parties and ensure patients and their data is protected. There are also important consent requirements not only for the patient, but for their authorized care-givers.
- 2) **Information systems are poorly connected.** The systems themselves are usually siloed , with data stored in multiple places in both structured and unstructured formats. It’s still a major challenge for most health systems to

---

<sup>1</sup> It is worth clarifying that some technologists will think of the term “Open Data” in the historical context of non-user data, e.g. exchange rates, but recently it has been used to encompass all user data, e.g. “Open Health” data as well as finance data. We will use this wider meaning in this whitepaper.

make the transition to Digital Health, such as migrating from paper to electronic health records or surfacing patient data to digital channels or third parties via APIs.

- 3) **There are a vast number of participants and entities in a health system<sup>2</sup>.** A given patient is interacting directly (and indirectly) with a wide array of entities and people that need to exchange data and services to provide the patient with care bespoke to their health requirements. This need is then multiplied by all participants in the system, patients with their own unique constellation of providers and records.
- 4) **There is more patient data & more desire for real-time access to it.** Medical devices and health apps gather ever more patient data, while certain health records like brain scans are individually data intensive. We are also seeing the early trends towards consumer managed genomics and prescribed digital therapeutics. Technology has both outpaced traditional methods of data storage and exchange, and radically scaled the demand for real time analysis across broad populations of patients
- 5) **New health technologies often require huge datasets.** Leading edge science and academic studies often require computer aided intelligence (artificial intelligence or machine learning) with access to large client datasets to detect anomalies and continuously improve algorithms and patient results, but meeting patient rights for privacy and consent based use of data for academic or diagnostic work can come into conflict. All of this information can then be combined with social determinants of health(e.g. environmental factors that affect one's health and quality of life.) essential data to minimize the bias that may occur when performing analytics
- 6) **Limited Digital Identity capabilities.** Digital identity capabilities that could help individuals assert their identity online are emerging, but still in their infancy. As Digital Identities are progressively issued by governments and enabled by private sector partners, they have the potential to help with a wide range of use cases including helping people assert their rights to access or to share health data. In the meantime, health technologists are limited to weak identity, verification and authentication capabilities that are generally available to their patients now.

This wide array of market participants together with the sensitivity of information and immaturity of the underlying information systems complicates the ability of all health ecosystems to move information and comply with regulation, even when there are

---

<sup>2</sup> The World Health Organization (WHO) defines a health system as follows, "A health system consists of all organizations, people and actions whose primary intent is to promote, restore or maintain health. This includes efforts to influence determinants of health as well as more direct health-improving activities. A health system is, therefore, more than the pyramid of publicly owned facilities that deliver personal health services."

effective policies and regulations. How are different governments and health systems trying to tackle the movement of health data around their domestic ecosystems? We'll take a global tour of the current and emerging health and identity policies and regulations, together with the standards bodies and interest groups working to deliver government policies and health outcomes. Our global tour will first turn to a few of the markets that are particularly active in the "consent-based" movement of patient records: the US, UK, Norway, and the EU. We'll also look at the global entities providing thought leadership on health standards (e.g. HL7, IHE) and domestic /regional entities providing local leadership (e.g. Sequoia Project, CAIRIN Alliance in the US)<sup>3</sup>.

Unfortunately, the consequences of poor identity capabilities have never been felt more acutely by the health sector. Few markets had the identity and health infrastructure in place they needed for national COVID19 testing and vaccination programs. These programs had to be built upon weak identity foundations, undermining our ability to meet public health goals at speed, and save lives. The challenges faced in COVID 19 are articulated in the whitepaper "Digital Identity in response to COVID-19," with contributions from the governments of Australia, Canada, Finland, Israel, New Zealand, Singapore, the Netherlands, the United Kingdom, and the World Bank (as an observer).<sup>4</sup> COVID laid bare the identity capabilities that are lacking in the health sector, but what is not commonly understood is that the same capabilities are needed to help people assert their identity in person and online for a wide range of other government and private sector use cases as well. Although the problems with identity transcend the health sector, so do the solutions.

In fact, some solutions to consent-based identity may be closer than even health experts expect. Our hypothesis is that the health sector can leverage the standards used by other sectors to reach their consent-based data and ecosystem requirements. APIs are the best way to open up consent-driven access to user data and are ubiquitous in the digital world. Much of the software that we use in our daily lives is powered by services delivered via APIs. The ability to get navigation directions, order delivery online, and communicate with email are use cases where data is provided via APIs. However many of these APIs are proprietary, although they may follow certain international standards, they are built to allow one company to use the services of another company. Such APIs are typically market driven and have a clear commercial rationale to be built and consumed by all parties, and are often built incrementally, `

---

<sup>3</sup> Sequoia Project: <https://sequoiaproject.org/> and CAIRIN Alliance: <https://www.carinalliance.com/>

<sup>4</sup> "Digital Identity in response to COVID-19," by the DGX Digital Identity Working Group.  
[https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx\\_2021\\_digital\\_identity\\_in\\_response\\_to\\_covid-19.pdf](https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf)

adding one counterparty at a time through bilateral relationships and commercial terms.

This paper will explore eco-system wide, consent-based data sharing initiatives in the financial services sector (Open Banking, Open Data), the identity sector (Global Assured Identity Network, EU Digital Identity Wallet/eIDAS<sup>5</sup>), and even the health sector itself (Norwegian *Health Network*) that address requirements similar to the health sector... at scale. We'll probe the API standards and operational approaches used to achieve scale, and which standards can meet health ecosystem requirements with little (or no) modification. Some of the key standards we'll explore are from the OpenID Foundation, a non-profit open standards body specialized in identity protocols. We'll look at how the Foundation's standards can leverage global security and identity standards and accelerate ecosystem-wide adoption, while domestic entities (be they public or private) retain their governance control (or "sovereignty") over their implementations. Perhaps most important to the health community, using existing standards can save time and money. Saving time can save lives. Reducing costs of "compliance" frees up resources to focus on other high impact initiatives, including initiatives to realize the full potential of consent-based health data sharing.

## Drivers of "Open Health"

### Government Mandates

As one might expect, government mandates are one of the key drivers of Open Health initiatives, mandates that place obligations on all participants in the health ecosystem so that all patients will benefit.

Benefits fraud are forcing both sectors to reassess the technology infrastructure and standards they need to meet user, government and society's needs.

### US

In 2006, the Institute of Medicine in the United States envisioned the concept of "Learning Health Systems," a patient centered framework to prioritize the needs and values of patients, to empower "source of control" in their own care. Learning Health Systems support the formation of communities of patients, healthcare professionals and

---

<sup>5</sup> <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

researchers who collaborate in routine healthcare settings to produce and use "big data" that generate research that in turn drives improvement at the point of care.<sup>6</sup>

In 2016, the US signed into law the 21st Century Cures Act (Cures Act). In the spirit of Learning Health Systems, the law is designed to promote innovation and accelerate the open exchange of health information nationally.

- The Cures Act final rule requires the healthcare industry to adopt standardized application programming interfaces (APIs) to help individuals to securely and easily access their health information, and introduces policies that support patient electronic access to their health information at no cost. The HL7 Fast Healthcare Interoperability Resource (FHIR®) standard will be required in all ONC-certified Electronic Health Record (EHR) systems by the end of CY 2022. Additionally, the final rule enhances the Office of the National Coordinator for Health Information Technology's Health IT Certification Program to advance interoperability, reduce operational burdens, and lower costs.
- The Interoperability and Patient Access final rule (aligning with the Cures Act final rule) specifies HL7 FHIR Release 4.0.1 programming interfaces (APIs) and additional services necessary to support secure and private exchange of patient information. These are the standards US health entities must implement against (to meet their compliance obligations), and in the future, their ecosystem-wide implementation will allow patients to easily access their claims and clinical information through the third-party applications of their choice.
- Trusted Exchange Framework and the Common Agreement (TEFCA) is a *voluntary program* that establishes a common technical infrastructure governing approach for different health information networks and their users to securely share clinical information with each other. Scheduled to go live in 2023, TEFCA will initially roll-out using globally established IHE profiles and HL7 C-CDA with a roadmap to incrementally implement HL7 FHIR by 2025. TEFCA will support the exchange of Personal Health Information (PHI) or Personal Identifying information (PII) for multiple exchange purposes (such as treatment, individual access services (IAS) or payment) aimed to improve access to health information.



## EU

The European Union released in the Spring of 2022 a proposal for the “Regulation of the European Parliament and of the Council on European Health Data space (EHDS)”<sup>7</sup> that addresses challenges to electronic health data access and sharing.” The EHDS envisions that natural person’s should control their electronic health data, and it enables researchers, innovators and policy makers to use this electronic health data in a trusted, privacy-preserving way. This legislation will build upon the voluntary aspects of the EU Cross Border Healthcare (CBHC) Directive to support the use of health data for specific purposes and promote the EU as a global standard for Digital Health.

Additionally the EHDS builds upon General Data Protection Regulation (GDPR)<sup>8</sup> and their proposed Data Act and Data Governance acts to provide specific rules that would cover purposes such as exchange of health data, portability of health data and the access of such data for secondary use.

The EHDS will also build upon the proposed European Digital Identity Act that includes the use of a Digital Identity Wallet that would provide mechanisms for both offline and online access to Identity information. The EU Digital Wallet (eIDAS 2.0) will likely be a key mechanism for EU residents to provide the consent and authorize the access and sharing of health data.

Not all government bodies are as highly regulated as the EU or US. For example, in Norway there is a legal requirement to share health information between legal entities when and if a health personnel has a legitimate interest, but their laws do not explicitly mandate how the health information should be shared.

See the “Country Initiatives” section for further context on Open Health implementations underway in Australia, Brazil, Canada, Hong Kong and Norway. Global community feedback is welcome to ensure full coverage of Open Health legislation and regulation.

## Privacy Laws and Data Protections

Beyond Open Health policies and regulation, the second key drivers are Privacy Laws and Regulations. As more and more social, business, and health transactions move online the importance of privacy and data protection is increasingly recognized.

---

<sup>7</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space  
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197>

<sup>8</sup> <https://gdpr-info.eu>

According to the United Nations Conference on Trade and Development (UNCTAD) statistics, 137 out of 194 countries they surveyed have put in place some form of legislation to secure the protection of data and privacy.<sup>9</sup>

In most countries, health information about a person is considered sensitive or special and often has required authorizations and/or consent requirements to access the data.

## US

In the US, health data rights are defined in a few ways, and they can vary by state:

- An individual has the right to obtain their health information (National).
- Authorization is a consent obtained from an individual [patient] that permits the disclosure of protected health information for other [defined] purposes]. (National, Health Insurance Portability and Accountability Act).
- “Informed consent” is an authorization or agreement to undergo a specific medical intervention (National).
- Consent may be required for 3rd parties (systems or humans) to access health information on behalf of the individual (State, laws vary).

## UK

In the UK, the National Health Service England is the owner of the health records. In this context, all policies are national:

- Patients have the right to see any medical report and share with other organizations but access to information which is deemed not relevant may not be shared.
- Consent for use is an opt-out based policy.
- Health information may be used for a number of purposes including improving quality of care and research.

## European Union

The GDPR states that consent must be freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.<sup>10</sup>

---

<sup>9</sup> Data Protection and Privacy Legislation Worldwide <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

<sup>10</sup> [https://en.wikipedia.org/wiki/General\\_Data\\_Protection\\_Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)

It is worth noting that the terms “permission”, “consent” and “authorization” are interchangeable, which clouds the distinction between what needs to be formally documented versus the essential computable elements necessary to authorize an online transaction. This makes alignment of technical standards more challenging, and further policy and regulation may emerge to refine the language.

## “Open Health” Initiatives

### A Global Movement

While there are commonalities across nations, the levels of maturity and roadmaps are fluid. This section details a representative sampling of countries to compare and contrast what health exchange across countries looks like today.

#### Australia

The Australian Digital Health Agency<sup>11</sup> mission is to improve health outcomes through the delivery of digital health services and systems. They provide key services such as Electronic Prescribing, Health identifiers for healthcare organizations, Healthcare provider and the patient, Secure Messaging, Clinical Terminology service and an opt-out online patient summary service called My Health Record. They are in the process of upgrading their digital health platform. As of 2022, their Initial focus is the upgrade/transition to a new Health API Gateway for exchanging and accessing health Information. It is a phase approach that will include a FHIR mobile gateway and improved B2B gateway services.

#### Canada

Canada Health Infoway (Infoway) provides a single view of patient information, via a viewer to support clinical applications, electronic medical records (EMRs), telehealth and other point-of-care solutions. Infoway recently implemented a national data exchange service, with FHIR-based API integration to prescriber EMRs, pharmacy management systems, and interops with registries and databases managed by the provinces and territories.

#### Hong Kong

---

<sup>11</sup> <https://www.health.gov.au/contacts/australian-digital-health-agency>

Hong Kong's Clinical Management system (CMS) is a comprehensive, integrated, interoperable EMR that supports transitions of care, prescribing medications, clinical ordering procedures and imaging, public health reporting, obtaining laboratory test results, viewing images, and safety alerts. The patient app allows patients to book appointments and reminds patients about attendance. In 2016, a territory-wide eHRSS was launched to permit public and private health sectors to share their patient data with explicit and informed patient consent. eHRSS is an opt-in system in which patients may voluntarily participate. The eHRSS is in the process of developing a patient portal to allow patients to access and enter their health data, and to define who can access their record.

#### Norway

In Norway, The government agency Norsk Helsenett SF (NHN) operates a closed membership based ecosystem, called the *Health Network* for all the legal entities that provide health care services. It offers health related IT-services like the national ePrescription, a national health record service and a death registration service. They are also working on a national *document sharing service* (XDS based). Additionally, the NHN established a national authentication service for the health sector (HelseID) built on OpenID Connect. This service is used for authenticating health personnel, and acts as a national federation gateway for all software that runs in the sector. Patient identities are created by commercial eID solutions and identity providers in the sector that offers a high level of assurance (LOA).

## Global Health Standards Bodies

Health information systems are generally governed by the following standards bodies and initiatives, standards bodies which address a wide range of Health Standards and Open Health is just one area:

### **ISO/TC (Technical Committee) 215 - Health Informatics (ISO 215)**

ISO 215 is responsible for the standardization in the field of health informatics, to facilitate capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system. With ISO representing over 160 countries and TC 215 having 66 participating and observing countries, it plays a vital international role in enabling the global reach of health information system standards. Open Health standards that are formalized in TC215 are likely to achieve wide scale adoption.

## **Health Level Seven International (HL7)**

HL7 is a not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. HL7, under a liaison agreement, may submit ANSI-approved or Standard for Trial Use (STU) specifications, for subsequent approval by the International Organization for Standardization (ISO) TC 215. Additionally HL7, ISO TC215 and other standards bodies are part of the Joint Initiative Council (JIC) that coordinates standards development efforts and works to develop a single standard in areas where that makes sense.

## **Integrating the Health Enterprise (IHE) International**

IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as Digital Imaging and Communications in Medicine (DICOM) and HL7 to address specific clinical needs in support of optimal patient care. The International Organization of Standardization (ISO) granted Integrating the Healthcare Enterprise (IHE) liaison D status to make standards-based IHE profiles a formal part of the ISO balloting process and ISO deliverables. IHE national deployment committees have been established in countries across the globe to conduct testing, education, outreach, collaboration with local health agencies and other deployment-related activities.

## **Comité Européen de Normalisation/TC (Technical Committee) 215 (CEN 215)**

CEN 215 is responsible for the standardization in the field of Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems and to enable modularity. This includes requirements on health information structure to support clinical and administrative procedures, technical methods to support interoperable systems as well as requirements regarding safety, security and quality. CEN has an agreement for technical co-operation with the ISO TC 215 through the Vienna agreement. The aim is to prevent duplication of effort and focus on the benefits of international standardization.

Other standards bodies, such as the World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF), IEEE Standards Association (IEEE SA), OpenID Foundation, and OASIS Open technical standards are often included as part of the downstream technical specification for the standard bodies mentioned above and may

have liaison agreements for other areas of interest within those bodies. Additionally, these efforts may reference privacy and security standards such as ISO 27001 and/or the NIST Cybersecurity Framework in the US.

A breakdown of countries and standards participation, and a summary of Open Standards in use today can be found in Appendix 1 and 2 respectively.

## Global “Open Health” Initiative G7 International Patient Summary

The health ministers of the G7 countries (Canada, France, Germany, Italy, Japan, United Kingdom, United States) have agreed to work towards adoption of a health data set that would enable patient access to health data and promote open health data based on the ISO International Patient Summary (IPS).<sup>12</sup> The ultimate goal is to agree on both technical and governance standards to enable the system-to-system transfer across international borders.

The ISO IPS was originally designed to be a minimum clinical data set for unplanned cross-border care. The G7 IPS initiative conceptually extends the ISO IPS to deliver a full clinical dataset transfer of information. For example, the G7 IPS standard will support both patient access and clinical use cases, such as patient authentication, patient ability to opt-in/opt-out, and clinician authentication prior to initiating B2B data exchange. While early G7 IPS releases will be “read only,” it is envisioned that “write access” will be needed for patient added information and details related to patient care.

One expected problem of the G7 IPS is that it may not be possible to share data across sub-national jurisdictions; additional processes may be needed to import information into the receiver’s system.

While the ISO IPS standard was not intended to be an implementation guide, HL7 published an Implementation guide in 2020 with examples of how the ISO IPS could be semantically constructed using FHIR resources, and the G7 IPS will leverage the HL7 Implementation Guide as a starting point in the effort.

An HL7 project called International Patient Access (IPA) is working on an Implementation Guide IG that is limited to the current HL7 IPS profile that recommends using the SMART-on-FHIR specification. The UK, US and Canada have demonstrated FHIR interoperability using the SMART IG but no known pilot or implementation as of this writing. Separately the EU has been piloting the CDA based ISO IPS profile across their member states/countries via their MyHealth@EU initiative. They anticipate

---

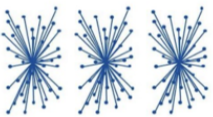


<sup>12</sup> <http://www.g7.utoronto.ca/healthmins/G7-Open-Standards-and-Interoperability-Final-Report.pdf>

implementation across 25 states by 2025. Not only is it encouraging that the EU Pilot work is an endorsement of the ISO IPS model; their implementation will inform the G7 and global deployment.

## Implementation Considerations

### Is the Trust Model Centralized, Federated, Decentralized or Mixed?

One of the first considerations is the kind of trust model suitable to the ecosystem's requirements. The diagram below gives a general description of the various types of Identity Management used within healthcare systems globally today. Often, there exists a hybrid between the different approaches via identity gateways (or middleware hubs) that provide security and access for brokered services, APIs, microservices, and end user devices.

IDENTITY MODELS	Centralized	Federated	Decentralized
			
TECHNOLOGY	<ul style="list-style-type: none"> <li>• ID/Password</li> <li>• Multifactor Authentication</li> <li>• Single Sign On</li> </ul>	<ul style="list-style-type: none"> <li>• OAuth</li> <li>• OpenID</li> <li>• SAML</li> </ul>	<ul style="list-style-type: none"> <li>• DLT</li> <li>• Cryptography</li> </ul>
CHARACTERISTICS	<ul style="list-style-type: none"> <li>• Identity fragmented across many enterprises</li> <li>• Enterprises control user data</li> <li>• Centralized data is a honeypot for cyber attacks</li> </ul>	<ul style="list-style-type: none"> <li>• Less fragmentation of login credentials</li> <li>• User information fragmented across many enterprises</li> <li>• Enterprises control user data</li> <li>• Centralized data is a honeypot for cyber attacks</li> </ul>	<ul style="list-style-type: none"> <li>• Identity can be portable across enterprises</li> <li>• User information in user's wallet or a secure cloud</li> <li>• Decentralized data limits data exposure on cyber attacks</li> <li>• Users control their data</li> </ul>

13

Like other verticals, Centralized Identity Management or Identity Access Management (IAM) suites are used by enterprises to authenticate health employees and authorize access to applications, APIs, and other resources. A hybrid federated / single sign on approach is often deployed to ease access for users by giving them the ability to access multiple systems across various sites both within and outside the enterprise.

<sup>13</sup> <https://www.citi.com/ventures/images/opinion/DI-1.jpg>; <https://www.citi.com/ventures/perspectives/opinion/digital-identity.html>

## Centralized

Centralized trust models for healthcare are very familiar to users and healthcare technologists, as are the problems they introduce. Users struggle to keep track of usernames and passwords, usernames and passwords can be lost or stolen and challenging to recover. Bad actors seek to compromise these authentication mechanisms to get access to the “honeypots” of data on the other side, data they can use for fraud, identity theft, or other cybercrime/ cyberwar purposes. Efforts to deploy multi-factor services (e.g. sending SMS authentication code out of channel) and phishing resistant methods of authentication (e.g. FaceID) are the primary tools that health service providers are implementing to mitigate risks, but these tools can also make it harder for users to access or recover their data. Today, most public and private health care services are structured in a centralized manner, with these “honeypots” across doctor’s offices, hospitals, health networks. It is worth noting that “screen scraping” solutions to aggregate health data has not gained material traction, as it had in financial services prior to the introduction of Open Banking (e.g. Intuit/Turbo Trust or Mint screen scraping), so the security issues related to screen scraping is less of an issue in the health vertical.

Centralized health systems can certainly enable Open Health ecosystems, but technologists and health executives should note that Open Health introduces additional risks and attack vectors. For example, weak authentication should not be used prior to allowing an End User or Clinician to authorize a transaction that will release data to an external third party.

## Federated

“Federated” in this paper can be viewed as an intermediate model, between traditional “centralized” and hierarchical authentication models on one side and the “fully decentralized” authentication models on the other side (e.g. W3C, Decentralized Identity Foundation and Trust over IP forums).

Federated models that use OAuth, SAML and OpenID Connect are also quite mature and familiar to health technologists, but there are some trends and risks worth highlighting. First it is worth noting that OpenID Connect (which is based on OAuth 2.0) is widely deployed across verticals and enables millions of applications and billions of end users to authenticate. Although as a standard it may be most widely experienced by users through social login solutions (e.g. Sign in with Apple, Login with Google, Login with Microsoft), it is also used at scale in enterprise to allow staff and administrators to access multiple applications via Single Sign On. In health, its used to share medical records amongst entities in the UK National Health Service, and amongst private



entities in the US. SAML is also a mature and longstanding solution for federated access to information especially by government and academic institutions. However, SAML is not actively maintained as a protocol, and reached its useful life from a feature set perspective, meaning there is risk for SAML users for the years ahead. The changes to browser primitives like removal of Third Party Cookies is an indicator that redirects used by advertisers (and that also compromise user privacy) are also likely to be changed by browsers (Chrome, Safari, Mozilla, Brave). SAML may well face “existential” threat issues from these changes, threats which OpenID Connect will also have to contend with, but which OpenID Connect has an active community of standards technologists to work on mitigations. Some entities are already starting to migrate from SAML to OpenID Connect, such as the Italian Government’s use of OpenID Connect Core and the Federation Spec for its online identity and national SPID services.<sup>14</sup>

Another trend is the potential for health systems to start migrating from OpenID Connect for the sharing of health data, to FAPI, a higher security profile from the OpenID Foundation. The FAPI profile is commonly used by Open Banking and Open Data implementations, but it has also been selected by the Norwegian Health Service (NHN) to move health data between the national health service and third party entities. More information on OpenID Connect and the Financial Grade API in the OIDF profile section.

## Decentralized

“Decentralized” is more than a buzzword, but less than a consensus, amongst technologists and legislators today, but for this whitepaper we need to look deeply at the scopes around the term “decentralized.” Just like the term “token” can mean very different things in discussions of OAuth access grants and cryptocurrency exchange, the term “decentralized” can take on very different meanings that are central to the design of any health care ecosystem, especially in trying to enable Open Health

**Location:** One scope is the decentralization from a location perspective, such as a distributed system and not a single, central compute system. A decentralized or distributed computer system could be a peer-to-peer or a client-server distributed system, both of which have been operational for decades. Under this scope, the global OpenID Connect ecosystem can be viewed as a decentralized system, with thousands of OpenID Connect servers (Identity Providers or IdPs), millions of clients (Relying Parties) and billions of End-Users. However, each individual OpenID Provider and Relying Party in this ecosystem is itself typically under the control of a single legal

---

<sup>14</sup> OpenID Connect in SPID: Guidelines Adopted [https://www.agid-gov-it.translate.google.it/agenzia/stampa-e-comunicazione/notizie/2021/12/06/openid-connect-sp-id-adottate-linee-guida?\\_x\\_tr\\_sl=it&\\_x\\_tr\\_tl=en&\\_x\\_tr\\_hl=en&\\_x\\_tr\\_pto=sc](https://www.agid-gov-it.translate.google.it/agenzia/stampa-e-comunicazione/notizie/2021/12/06/openid-connect-sp-id-adottate-linee-guida?_x_tr_sl=it&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc)

entity. The main exception is a Self-Issued OpenID Provider (Self-Issued OPs), where the End-User has their own OpenID provider (e.g. on their device).

**End User Ability to Bring their Own Identifiers to the Credential Issuers:** Another Decentralized scope is whether the End-User is able to bring their own identifiers to the Credential Issuers and Verifiers instead of having identifiers assigned to them by the third party Identity Providers. W3C Decentralized Identifiers (DIDs) are being mentioned the most in this context of identifier decentralization, while there are options to use other types of identifiers that are not DIDs. At the moment, there are 40+DID methods and this number is likely to grow before use cases and implementations narrow the field to a smaller range of DIDs that are used in the majority of implementations.

**End-User Ability to Present credentials to Verifier:** There is also a Decentralized scope of the End-User's ability to present credentials to the verifier, without the verifier having to contact the Credential Issuer directly. W3C Verifiable Credentials (VCs) are being mentioned in this context of decentralization of the credential presentation.

**Independence from a Single Entity's Control:** Finally, there is Decentralized from a control perspective, which means not depending on one single body controlling access to the ecosystem. The "NASCAR problem" and "wallet wars" are usually mentioned in this context. It depends on the use-case and level of assurance of the required credentials whether any entity is allowed access to the ecosystem, or only certified or otherwise "allowed entities" can access the ecosystem. OpenID Connect Core already enables this range of access control within the available technology, but many relying parties do not enable complete user choice of OpenID Providers. Realizing a completely open and fully decentralized ecosystem might require some technical changes to certain software components (such as browsers and mobile Operating Systems), and potentially even regulation.

### **Will the Health System Leverage Verifiable Credentials?**

Verifiable credentials are a promising technology for health use cases. For a deep dive on Verifiable Credential use cases, standards and to harmonize them with OpenID Connect, refer to the "OpenID Connect and Verifiable Credentials" 1st Editor's Draft.<sup>15</sup> For the health audience, we extract some key insights such as insights on the myths common to discussions of this technology in Appendix 3.

---

<sup>15</sup>[https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper\\_OpenID-for-Verifiable-Credentials\\_FINAL\\_2022-05-12.pdf](https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf)

## Identity Profiles

Regardless of the trust model used in the ecosystem, such as Centralized, Federated or Decentralized there is typically a need to specify how the implementation will be configured and allow interoperability between the entities (interoperation maybe within an entity, or across numerous entities.) Security profiles provide a means to use standards and protocols in a consistent manner, to simplify access and promote greater interoperability between systems and users. Identity profiles focus on the technical specifications to authenticate and authorize user that have access to sensitive information, and often provide best practice guidance to ensure the data access is not compromised by malicious actors.

Below is a representative list of profiles specifically used to support FHIR APIs:

- The IHE Internet User Authentication (IUA)<sup>16</sup>, a profile based on OAuth 2.1, is an essential part of the IHE Mobile Health Sharing Document Sharing (MHDS) specification. The IHE MHDS is a draft a collection of profiles that include Identity (patient, author and organization) and Authorization Management (Access control and consent)<sup>17</sup> that supports FHIR and is designed to help health IT implementers move from the legacy SOAP SAML based Cross Domain Document Sharing (XDS) and HL7v2 profiles in use today.
- SMART App Launch (aka SMART-on-FHIR) specification includes private Key JWT authentication, client authentication, authorization to launch an app within an electronic health record (EHR), backend/backchannel authorization and Token Introspection<sup>18</sup>. The use of SMART on FHIR is required in US regulation for Electronic Health Records systems governed by the ONC Certification Program.
- The OpenID HEART profiles focus on patient access and control of their own health and wellness information. The HEART profiles were purposefully designed to align with SMART-on-FHIR to ensure developers that supported the HEART profiles for patient/consumer based access could be used in tandem. The HEART profiles are referenced in the HL7 FHIR Security guidance as potential use for access control decisions.
- The Unified Data Access Profiles (UDAP) was specifically defined for US healthcare interactions for both FHIR based B2B Provider/Payer and B2C exchanges. The profiles include JWT-Based Client Authentication, Tiered OAuth

<sup>16</sup> [https://wiki.ihe.net/index.php/Internet\\_User\\_Authorization](https://wiki.ihe.net/index.php/Internet_User_Authorization)

<sup>17</sup> <https://profiles.ihe.net/ITI/MHDS/volume-1.html#1506-mhds-cross-profile-considerations> Mobile Health Document Sharing 2.3.0 Trial implementation Use

<sup>18</sup> <http://www.hl7.org/fhir/smart-app-launch/> SMART App Launch

for User Authentication, Mutual TLS Client Authorization, Client Certifications and endorsements, JWT based Client Authorization and publishing of metadata. UDAP has been implemented in US as part of the draft Carequality FHIR Implementation Guide and the HL7 CARIN Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®)<sup>19</sup>. The CAIRN IG for Blue Button has been referenced as an option in the US Interoperability and Patient Access final rule for health insurance payers to use to satisfy the requirement to release health claims information.

[For each of these profiles, work has evolved independently. This is partly due to the fact that as the FHIR protocol has matured], additional use cases are identified that could benefit from the use of FHIR. Often, instead of re-using and extending existing profiles and resources, additional FHIR resources and profiles are created to support them<sup>20</sup>. In Appendix XX, in preparation for this paper, we did a mapping of underlying standards and protocols across the various Identity based implementation drafts and guides to gauge the commonalities and differences across profiles. The profiles generally align with minor evolution in the standards chosen at that time. These decisions are most often made based on the timing and maturity of standard (moving from draft to standard) and experience gained from implementer working with the profiles in real time. If you then compare and align what has been done in the health sector side by side with the standards and protocols used within the FAPI work for Open Banking (detailed later in the document), note the incremental, but substantive changes from FAPI 1 to FAPI 2 that have occurred to address lessons learned from implementing FAPI 1 at scale.

## Consent

Consent is a form of permission that is used to determine authorization and access control decisions. The legal requirements to document consent are quite different from the scopes, claims and/or access policies that are implemented to enforce the consent and delegated access to health information. To complicate matters, in certain situations, regulations may be in place that would override the authorization prohibiting or severely restricting the type of information that may be released. Or vice-versa, in opt-out or implied consent scenarios, the evidence of consent may not be necessary. The variability of profiles also extends to the choices made in the way consent may be expressed.

---

<sup>19</sup>CARIN IG for Blue Button <http://hl7.org/fhir/us/carin-bb/>

<sup>20</sup>FHIR Profiliferation <https://www.medrxiv.org/content/10.1101/2022.03.09.22272163v1.full>

One approach is to use the FHIR consent resource. The resource is currently in Trial Use with limited testing. The current iteration intends to cover Privacy Consent Directives, Medical Treatment Consent Directives, Research Consent Directives and Advance Care Directives but as of this writing, HL7 has only modeled the Privacy Consent Directive which focuses on the authorization to collect, access, use or share health information. The FHIR consent is considered legally binding if it can meet the requirements of an enforceable contract. Enforcement is not in scope for the resource but it is expected that the Consent Resource could be used to define enforcement policies via other standards such as XACML, OAuth or UMA.

SMART-on-FHIR profiles offer considerations for consent but delegate actual responsibility to the developer to determine how to implement. This opens the possibility for great flexibility and variability between implementations and use cases.

The HEART profiles defined a baseline set of general access (read/write/\*), confidentiality, sensitivity and break the glass scopes and a set of UMA 2.0 claims that can be used across domains to represent common access conditions.

Carequality<sup>21</sup>, a national health information exchange framework that is also leading the development of the TEFCA Qualified Health Information Network (QHIN) Technical Framework (QTF), has released a draft Carequality FHIR Implementation Guide<sup>22</sup> that leverages UDAP and defines an additional “carequality” authorization extension object. Their IG implements OID base access consent policy (acp) assertions that include OIDs for consent and various patient permission. The authorization extension object includes a “purpose\_of\_use” string for the data requested and may include consent based acp assertions and their associated acp\_reference containing an array of FHIR DocumentReference pointing to the underlying documentation or FHIR Consent resources.

There are additional coordinated efforts outside the health sector that are focused on consent that may be worth tracking. ISO/IEC 29184:2020<sup>23</sup> is a specification that controls the format of online privacy notices and the process of asking for consent in cases where explicit consent and/or notice is required. The work was informed by the Kantara Initiative, Inc Consent receipts. ISO/IEC TS 27560<sup>24</sup> – Privacy technologies – Consent Record Information Structure is an initiative under development that proposes to develop an extensible data structure that can be used to support the provision of a

---

<sup>21</sup> <https://carequality.org>

<sup>22</sup> <https://carequality.org/wp-content/uploads/2020/12/Carequality-FHIR-Implementation-Guide.pdf>

<sup>23</sup> <https://www.iso.org/obp/ui/#iso:std:iso-iec:29184:ed-1:v1:en>

<sup>24</sup> <https://www.iso.org/standard/80392.html>

consent, exchange of consent between systems and manage the lifecycle of consent. There are parallel efforts occurring in the newly formed Kantara Initiative - Advanced Notice & Consent Receipt WG<sup>25</sup> and the Trust Over IP (TOIP) Notice and Consent Task Force<sup>26</sup> to contribute to the structure of the international standard and potentially leverage Decentralized Identifiers and Verifiable credentials.

## Conformance and Certification

If one of the first considerations for an ecosystem is the level of centralized versus decentralization of the ecosystem, and the second is the selection of standards including profile and consent configuration, the last consideration is how to ensure conformance and interoperability amongst all the participants.

There are a number of certification testing efforts underway in the Open Health domain, both mandatory and voluntary, that are being managed today. One of the major issues is the limitation imposed on these tools by restricting options based on various regulations. As a result, multiple versions of the tools need to be implemented in order to test conformance.

Amongst Open Banking and Open Data implementations the best practice is to mandate conformance and certification to standards, regardless of whether the ecosystem is public or private. Even with a clear and stable standard, interpretation of a standard opens up risks of variation in code that cause extensive development and operational burden to debug, and failure to conform can open material security risks as well. The whitepaper on “Open Banking, Open Data, and the Financial Grade API” is an excellent primer on the challenges faced by the financial services community implementing markets like the UK, Brazil and Australia, and the risks and benefits of formal conformance and certification processes.

Although both the Open Data and Open Health movements are in their infancy, learnings from Open Data may help health technologist and health administrators when crafting their ecosystem wide system requirements.<sup>27</sup>

---

<sup>25</sup> <https://kantara.atlassian.net/wiki/spaces/WA/overview?homepageld=2916356>

<sup>26</sup> <https://wiki.trustoverip.org/display/HOME/Notice+and+Consent+Task+Force>

<sup>27</sup> [https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper\\_Open-Banking-Open-Data-and-Financial-Grade-APIs\\_2022-03-16.pdf](https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf)

## Why Choose OpenID Foundation Security Profiles

OpenID standards are frequently selected for Centralized, Federated and now for Decentralized solutions as well. However, health technologists are often unfamiliar with the full range of optionality in the specifications, and their knowledge may be overly colored by social login or enterprise implementations they have used in the past.

First it's important to note that Foundation standards are already being used for Health ecosystems today. As discussed earlier, markets like the US and UK are using OpenID Connect Core and it is referenced in the SMART-on-FHIR, MHDS and UDAP profiles to share clinical information via FHIR APIs, so it's already part of the health community's standardized approach. Additionally the Norwegian Health Service (NHN) has selected the OpenID Foundation Financial-grade API (FAPI) as core to their *Health Network* initiative and have successfully collaborated with EPIC, their national health system provider, to implement FAPI.

We are also at the cusp of seeing convergence between national Digital Identity, Open Health and Open Data efforts. For example, in Europe the European Health Data Space (EHDS) proposal for regulation seeks to "Put people in control of their own health data, in country and cross-border" and the "...EHDS builds upon the new proposal on the European Digital Identity 22 with the improvements in the domain of electronic identification, including the Digital Identity Wallet. This would allow better mechanisms for the online and offline identification of natural persons and health professionals."<sup>28</sup>

The EU Digital Identity "Architecture Reference Framework" (ARF) will in turn incorporate many global standards like ISO 18013-5 mobile driving license (which includes OpenID Connect, and has the potential to extend to government issued national IDs and passport), and W3C Verifiable Credentials (which can align with OpenID Connect for Verifiable Credentials family of specs).

Similarly the Australia legislation on Consumer Data Right, cuts across financial services, utilities and telecommunication networks, and it will not be surprising if these rights extend to Digital Identity and Health as well. There is a material benefit to policies and implementations that address residents' needs across use cases, and are not overly constrained by the authority of one government department.

---

<sup>28</sup> European Health Data Space [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_2711](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711)



With all the activity underway both within and adjacent to the health community, all this innovation, policy and implementation work is a fertile environment for convergence...and a high risk of divergence from global standards. There are several known benefits of global standards, such as they can save implementor resources and time to market, and implementation experience security issues can be solved by many instead of a few people. One of the most important benefits of the OpenID Foundation's open standards based approach, is that anyone can use them at no cost, and no domestic entity or government authority loses their ability to control their respective local implementation by selecting them. This balance of benefiting from global standards while retaining control (or "sovereignty") is one of the key reasons many Open Banking/Open Data ecosystems are selecting the Foundations standards today.

For those that are unfamiliar, we will further clarify who the Open ID Foundation is and what they do, and which Foundation standards meet Open Health requirements.

## What is the OpenID Foundation

The OpenID Foundation is a global, non-profit standards body whose vision is to help people assert their identity wherever they choose. Its mission is to lead the global community in creating identity standards that are secure, interoperable, and privacy preserving. All working groups operate openly, and anyone can contribute without paying fees. Decisions on specifications are consensus-led, and all standards and test suites are freely available for anyone to use under the protection of the OpenID Foundations's IPR agreement. The Foundation is primarily funded through three sources, roughly equally: membership, certification fees, and directed funds.

The foundation also offers support for implementers in several ways such as:

- **Due diligence:** We seek to ensure members understand OI DF standards and the benefits of implementing them. We also actively share sharing OpenID Foundation and member learnings, insights that tend to resonate especially well with government partners, and managing entities building new networks.
- **Liaisons with partners:** Sometimes government partners benefit from the foundation developing a liaison with a particular global, regional or national partner, like a standards body or governance entity. We enter into liaisons and partnerships with other standards bodies, non-profits, and private entities that help the foundation deliver on its mission.
- **Certification:** The foundation offers test suites on our mature standards at no cost, and nominal fees for self-certification by Identity providers, vendors, relying parties and others. Our certification program has been selected by government



partners like the UK and Brazilian authorities to ensure their ecosystem participants conform to their requirements. We are also developing a 3rd party licensing model, to create a formal arrangement with local entities that need to combine certification on OIDF standards into a single operational process (e.g. functional and operational requirements that form part of a wider ecosystem implementation of Open Health). In general, the foundation is keen to partner closely with implementers to identify bugs and issues so that the global community benefits from any issues detected, and the certification program is a great way to stay in regular communication with local implementers.

- **Local Profile development and maintenance.** We encourage partners to seriously consider developing their profile in partnership with the OpenID Foundation, and leaning on the foundation to maintain it. This will allow the local entity to maintain control over the profile and decisions, while leveraging the expertise of the foundation in development, maintenance and testing for the profile. This approach saves local entities time and money at the start and overtime, reduces security risks of divergence, and reduces the risk of technical barriers to achieve cross border interoperability over time.
- **Interfaces with other standards.** The Foundation also helps members understand how the foundations specifications (such as adding on OIDC for Identity Assurance, or Shared Signals and Events to a FAPI implementation), and interfaces with other liaison partner standards like FIDO, W3C VCs, or ISO 18013-5 Mobile Driving Licenses.

All market participants are warmly encouraged to join the Foundation to help deliver on the OpenID Foundation's vision and mission. Participants can join as governments, non-profits, private entities and as individuals. More on the OpenID Foundation at [openid.net](https://openid.net).

## Overview of Relevant OpenID Foundation Security Profiles

### OpenID Connect

OpenID Connect Core was published by the OpenID Foundation in 2014 as an “identity layer on top of the OAuth 2.0 protocol”. It made it possible for users to perform “social logins” by “signing in” and verify their identity to third party services. It has been

implemented by Google, Microsoft, Apple and others and is used by billions of users across millions of applications for B2C, B2B and B2B2C use cases and verticals.

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol, including additional security mechanisms. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End User. OpenID Connect is API-friendly, and usable by native and mobile applications, so clients of all types, including Web-based, mobile, and JavaScript clients, can request and receive information about authenticated sessions and end-users. The standard also defines optional mechanisms for robust signing and encryption, and it is extensible, allowing participants to use optional features such as encryption of identity data and discovery of an End-User in an interoperable and REST-like manner. The standard is very mature, and most implementations today use profiles based on OpenID Connect Core.

The OpenID Connect standard is also referenced in other international standards such as (ISO, IETF, etc) and it can be implemented in conjunction with other security standards, such as FIDO, for end to end security.

It is worth noting that many health systems have legacy SAML implementations, which has historically been able to meet ecosystem requirements. The key challenge for SAML implementers is whether they will be able to maintain their SAML implementations as is, or will eventually need to migrate away from it. One reason is because SAML is not actively maintained, and new features are not being developed. This is felt in the lack of multi-channel capabilities, and “workaround solutions” required to adapt SAML infrastructure with the multichannel requirements of users today, and the potential “existential threat” of browsers removing redirect web primitives that SAML relies upon (as so the advertisers the browsers are trying to constrain in the interests of user privacy).

## HEART

HEART (Health Relationship Trust) is a set of OpenID Connect profiles that enables patients to control how, when, and with whom their clinical data is shared. The HEART model gives patients control over how their own data is shared, and it defines the interoperable process for systems to exchange patient-authorized healthcare data using FHIR, OpenID Connect, OAuth and UMA (User-Managed Access).

The goals of the HEART profiles are to :

- Enables organizations and other entities to electronically determine whether requests for data are valid (ie, have been authorized by the patient) and what data the requesting entity is authorized to obtain.
- Creates a protocol for managing both sharing of permissions and data that adheres to the highest levels of security and privacy. In the process, both patients and providers can trust that the data is authorized and accurate.
- Supports, and integrates with, systems that allow patients to set up permissions and authorizations for sharing their clinical data to ensure that their data is only shared with individuals, institutions, and apps that they choose.

The HEART profiles have had some moderate success and are referenced as a viable option for access control in the HL7 FHIR Security guidance. That said, the profiles were developed a little ahead of its time, ahead of regulatory obligations, and will soon be slightly out of sync with other profiles. For example the pending updates to SMART-on-FHIR 2.0 made changes to the scope definitions in the profile that are not backwards compatible. While use of the HEART profile may suffice for mandated implementation in the US in the near term, the existing profiles would need to be updated to keep pace with those changes.

To obtain the full benefit of Open Health, entire ecosystems need to deploy the same standards, and crucially the user-consent based capabilities like those in HEART. It may be time for the OpenID Foundation and health technologists to assess the value of maintaining the existing HEART profiles or capture and channel requirements to the appropriate OIWF WG, e.g. FAPI WG, OIWF for Verifiable Credential Sub WG. This would need to be a coordinated effort with relevant international, regional and national health standards bodies, and require work with public and private sector leaders to achieve widespread adoption and compliance through conformance and certification policies. By taking these steps, we can truly empower patients, clinicians and academics while respecting patient privacy and security needs.

## FAPI

OpenID Connect Core was published by the OpenID Foundation in 2014 as an “identity layer on top of the OAuth 2.0 protocol”. It made it possible for users to perform “social logins” by “signing in” and verify their identity to third party services. It has been implemented by Google, Microsoft, Apple and others and is used by billions worldwide for B2C, B2B and B2B2C use cases across verticals. As part of the design of OpenID Connect additional security mechanisms were specified that increased the security of OAuth 2.0.

In 2016 the OIDF Financial API Working Group was formed with the specific goal of providing security recommendations and specifications to enable secure APIs in financial services. The working group soon focused on 2 security profiles, now referred to as FAPI 1.0 Baseline and FAPI 1.0 Advanced. These 2 profiles built on the work of OAuth 2.0 and OpenID Connect to provide an opinionated secure profile of OAuth 2.0 suitable for use in financial services.

FAPI significantly reduces costs for ecosystem participants by introducing economies of scale. Since the standard is built on a family of RFCs, there is high “out of the box” vendor support, and the FAPI security profiles have been implemented by most vendors in the Identity and Access Management industry. This means less costly customization or bespoke work is required if an ecosystem chooses FAPI, and it also reduces the vendor lock-in and switching costs downstream. The maturity and wide adoption of the standard also means there are multiple open source libraries that implement OpenID Connect and FAPI that can be used by data receivers in an ecosystem to accelerate implementation. Last, the global community of experts working on implementations and sharing findings serves to not only reduce security and operational risks, it also reduces operational costs of maintaining bespoke standards.

FAPI was designed to serve higher risk use cases than OpenID Connect, and the FAPI 1.0 has been through a formal security analysis by the University of Stuttgart. However, within the FAPI family of specs there are also many choices, such as Baseline and Advanced, to help ecosystem thought leaders to perform “progressive profiling.” In short, the standards themselves give serious consideration of foundation overlays for different vertical use cases and international interoperability. This allows for standards that are commensurate to the security needs and security posture of any given regime, as well as a way to modularise “fit for purpose” within legal and regulatory frameworks. In short, the standards allow local sovereignty and control of profile configuration and governance, while preserving the benefits of international standardization for operational, security and interoperability benefits.

Originally the FAPI Working Group was focussed on APIs within financial services and it was called the Financial API Working Group. However the name was changed to “financial grade” API to reflect the fact that its security profiles are suitable for APIs in other verticals beyond finance. The foundation is focusing on all aspects of Open Data including finance, insurance, health, and government use cases. Some use cases like insurance may not require any changes to the FAPI standards (as per Australian Consumer Data Standards). This in turn drives down the cost for countries looking to roll-out a standardized security framework across many industries in their economy whilst increasing speed to market.

The FAPI Working Group is taking learnings from the implementation of FAPI 1.0 to create a framework for FAPI 2.0 that will provide all of the standards necessary to implement an Open Data ecosystem. This includes work on new specifications such as Grant Management and Dynamic Client Registration as well as deployment advice. Given some markets are adopting the FAPI 2.0 standards this year, and the OIDF is progressing Security Analysis on both the FAPI 2.0 baseline & advanced specifications starting March 2022. Australia is planning a transition to FAPI 2 in 2023, and other new ecosystems may want to consider starting with FAPI 2.0. The OpenID Foundation is collaborating again with the University of Stuttgart to perform a security analysis of FAPI 2 baseline and advanced to finish in 2022. It is also the expectation of the FAPI WG and key government partners like the Brazilian Central Bank and the Australian Data Standards Body that the FAPI Security Profile does not need to be changed in a material way to support other verticals like Open Insurance (Brazil) or Utilities/ Telecom (Australia). For more information on the FAPI standard, see the "Open Banking, Open Data and the Financial Grade API" whitepaper.<sup>29</sup>

## OpenID for Verifiable Credentials

There are many myths about Verifiable Credentials which confuse even the expert identity technologists working on standards. See Appendix 3 to unpack these myths, as some health technologists may be struggling to parse the "signal from the noise."

This paper seeks to focus on the "signal" by highlighting the convergence work the OpenID Foundation is doing to align OpenID foundation standards with Verifiable Credentials and other credential types like ISO 18013-5 Mobile Driving Licenses to maximize the benefits of all three standards. Just as the identity community is intrigued by this work (and joining the OIDC for Verifiable Credentials in large numbers), so can health technologists benefit from this work.

The OIDC protocol was designed as an authentication layer on top of OAuth to enable the release of Identity claims from an OIDC authorization server to the Relying party client to provide identifying information about the user accessing the Relying party's application or service.

Now, User-Centricity is evolving even further to give the end user more control over what Identifying information may be released, thus improving privacy and portability over

---

<sup>29</sup> [https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper\\_Open-Banking-Open-Data-and-Financial-Grade-APIs\\_2022-03-16.pdf](https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf)

their identity information. We'll go through all four specifications, each of which addresses a unique use case.

### **OpenID for Verifiable Credentials (OpenID4VC)**

Using OpenID for Verifiable Credentials protocols, the End-Users can now directly present identity information to the Relying Parties, and this specification covers Self-Sovereign Identity, Decentralized Identity, and User-Centric Identity use cases. This architecture enables the End-User to directly receive credentials from the Issuer and directly present them to the Verifier using verifiable credentials. It is important to note that verifiable credentials are not only limited to credentials expressed using W3C VC-DATA-MODEL, but the standard allows for identity credentials expressed using other data models such as ISO 18013-5 Mobile Driving Licenses. The following are the key features of OpenID4VC Family:

- Simplicity
- Developer familiarity and friendliness
- Leverages deployed OpenID Connect infrastructures (facilitates verifiable credentials adoption)
- Security
- Flexibility regarding identifier (e.g. DID methods), credential formats, cryptographic schemes, and revocation schemes

### **SIOP v2**

The Self-Issued OpenID Provider (Self-Issued OP) was already part of the OpenID Core specification (this version is designated as SIOP v1). It enabled End-Users to be in control of the identity information and signing keys. Using the Self-Issued OP, an End-User could authenticate using a self-signed ID Token that was signed using the key material controlled by the End-User.

The emerging SIOP v2 aims at adjusting SIOP v1 to the challenges of modern verifiable credentials applications. It introduces the following capabilities:

- Support for DIDs in addition to the raw JSON Web Keys as End-User identifiers
- Support for Dynamic Self-Issued OP discovery
- Support for invoking Self-Issued OP via HTTPS URLs in addition to the custom schemes such as "openid://". This enables the use of deep/app/universal links on modern smartphone operating systems and web wallets.

- Support for all OpenID Connect Flows, e.g. authorization code flow, which allows cloud/web wallets to leverage the advanced security features and capabilities in comparison to the traditional “OIDC implicit” flow utilized by SIOP v1.
- Support for “cross device” flows, where the End-User can start the presentation on a different device than where the credentials will be accessed from, in addition to the “same device” flows
- Support for OpenID Connect Registration metadata for the management of wallets. This enables interactions among pre-registered and verified RPs and Self-Issued OPs, which is an important enabler for regulated verifiable credentials schemes (e.g. eIDAS 2), in addition to ad-hoc interactions.

### **OpenID Connect for Verifiable Credential Issuance (OIDCVCI)**

OIDCVCI defines an API designated as a Credential Endpoint and corresponding OAuth-based authorization mechanisms for issuance of verifiable credentials, e.g., in the form of W3C Verifiable Credentials. This allows existing OAuth deployments and OpenID Connect OPs to extend their service and become credential issuers. It also allows new applications built using Verifiable Credentials to utilize OAuth and OpenID Connect as integration and interoperability layer.

### **OpenID Connect for Verifiable Presentations (OIDC4VP)**

OIDC4VP extends OpenID Connect with the ability to request and present verifiable credentials. It therefore introduces the new “VP Token” to convey verifiable presentations and integrates the DIF Presentation Exchange into the “claims” request parameter to specify the RP’s requirements regarding the credentials to be presented as well as to help the verifier process the result.

## **Shared Signals and Events**

The Shared Signals and Events (SSE) Framework from the OpenID Foundation improves API efficiency and security by providing privacy-protected, secure webhooks for zero-trust environments.

It is in use by some of the largest cloud services to communicate security alerts and status changes of users, continuously and securely to prevent and mitigate security breaches, and these providers have proven its efficacy within their own implementations and across entities. In other words, these standards can act like the nervous system for a network or “network of networks” to manage risks and inform decision making in real time.

Just as the SSE standard has been adopted by leading digital platforms and vendors, health technologists will want to consider this standard to ensure their Open Health implementations have a “nervous system” to protect movement of patient data between parties.

For more information on Shared Signals and Events and the underlying Continuous Access Evaluation Protocol (CAEP) and Risk Incident Sharing and Coordination (RISC) specifications, refer to <https://openid.net/wg/sse/>.

## Other OpenID Foundation Working & Community Groups

The OpenID Foundation is also working on identity standards interfaces with IoT standards, standards to enable identity networks to interoperate with OIDC for Identity Assurance, and is an active founding member of the Global Assured Identity Network and the GAIN Proof of Concept Community Group, more on OIDC for IA and GAIN in Appendix 5, and other Foundation efforts at [openid.net](https://openid.net).

## Other Standards & Tradeoffs

[Add section on other standards and relative tradeoffs? For a balanced view of relative strengths, where there may be duplication of effort and informed views from Foundation]

## Recommendations

As the 1st Editor's Draft, these are the editor's initial recommendations for feedback from the health community.

### Partner Organizations

- IHE
  - IHE & OpenID Foundation to explore a liaison agreement to evaluate potential role of OpenID Foundation standards to enable Open Health, domestically and globally.
  - OpenID Foundation to participate in regional “connectathons”
- HL7
  - HL7 and OpenID Foundation to explore a liaison agreement to evaluate potential role of OpenID Foundation standards to enable Open Health, domestically and globally.
- Joint Initiative Council

Gail Hodges 6/21/2022 2:03 AM

**Comment [1]:** What other standards and pros/cons might we need here? or are we covering this in the profile and consent sections above?



- IHE & OpenID Foundation to explore a liaison agreement to evaluate potential role of OpenID Foundation standards to enable Open Health, domestically and globally alongside other key participants IHE, ISO and HL7.
- Trusted Exchange Framework Common Agreement (TEFCA) - USA
  - Explore OpenID Foundation and TEFCA Pilot with existing architecture
  - Explore OpenID Foundation contributions to the FHIR API 2 year roadmap
- CARIN Alliance - USA
  - Explore OpenID Foundation and CARIN Pilots with existing architecture
- EU Decentralized Health (EU)
  - Build on OpenID Foundation brief to EU Digital Identity/ eIDAS expert group to support EU legislative effort[insert name]
  - Explore partnering with EU country for EU Identity Pilot
- [Canadian pilot - Insert name of initiative and timeline]

### **OpenID Foundation Working Groups**

- Solicit OIDF Board, member, and liaison partner feedback on the reformation of HEART WG as the Health WG with a mission to deliver on 5 goals:
  - Manage liaisons with key global and national health standards bodies including HL7, IHE, TEFCA.
  - Determine if there is value in maintaining the existing HEART profiles or capture and channel requirements to the appropriate OIDF WG, e.g. FAPI WG, OIDC for Verifiable Credential Sub WG.
  - Maintain any other health profiles, review health related certification tests, and support 3rd party licensing activities in partnership with the OIDF certification team.
  - Facilitate advocacy for OIDF standards in the Health community.

### **Open Questions**

- What privacy and security concerns are truly unique to healthcare?
- Can the success with independent testing for FAPI and Open Banking be extended to the Health sector?

## **Conclusion**

Open Health has arrived and is here to stay. Delivering personalized and leading edge medical care while empowering patients with control of their health data has never been more achievable, but the manner in which ecosystems implement Open Health can

have a profound effect on user control, costs, innovation, privacy and security. Through use of mature global standards and certification programs, health technologists can architect their implementations, domestic ecosystems, and health “networks of networks” to interoperate. Public and private ecosystem leaders can maintain their governance authority, while leveraging standards and security models that are proven to unlock the movement of data. By working together, the health, identity, and government communities can leverage our respective strengths and focus our resources to build global scalable and interoperable infrastructure that empower patients and deliver transformational care.

The OIDF warmly welcomes individuals, companies and organizations to join the OpenID Foundation to support the work on the all of our standards ([www.openid.net](http://www.openid.net)) and ensure they are fit for purpose, and we close gaps in the interfaces with other global and local standards.

If you are working for an Open Health initiative and would like to learn more about the OpenID Foundation we can support your goals both domestically and internationally then please reach out to [director@oidf.org](mailto:director@oidf.org), we look forward to working with you.

## Appendix 1: Country & Regional Standards Participation

Below is a table representing the countries that actively participate in health related standards development. To the left of the countries are global forums and initiatives that have interest in global health concerns and the countries that participate in them.

G7	G20	GDHP	Countries	CEN TC 251	ISO TC 215	HL7 Affiliates	IHE Deployment
	x	x	Argentina		observing	x	
			Armenia		observing		
	x	x	Australia		participating	x	x
		x	Austria	x	participating	x	x
			Bahrain		observing		
		x	Belarus				
			Belgium	x	participating	x	x
	x	x	Brazil		participating	x	x
			Bulgaria	x	observing		
			Burundi		observing		
x	x	x	Canada		participating	x	x
		x	Chile			x	
	x		China		participating	x	x
			Colombia		observing		
			Croatia	x	observing	x	
			Cyprus	x	observing		
			Czech Republic	x	observing		x
			Denmark	x	participating	x	
			Ecuador		observing		
			Egypt		participating		
		x	Estonia	x			
			Ethiopia		participating		
			Finland	x	participating	x	x
x	x		France	x	observing	x	x
x	x		Germany	x	participating	x	x
			Greece	x		x	
		x	Hong Kong		observing		
			Hungary	x	observing		
			Iceland	x			
	x	x	India		participating	x	

	x	x	Indonesia		observing		
			Iran, Islamic Republic of		participating		
			Ireland	x	participating		
			Israel		participating		
x	x	x	Italy	x	participating	x	x
x	x	x	Japan		participating	x	x
			Kazakhstan		participating		
			Kenya		observing		
	x	x	Korea, Republic of		participating	x	x
			Latavia	x			
			Lithuania	x			
			Luxembourg	x	observing		x
			Malaysia		participating		
			Malta	x			
	x		Mexico		observing	x	
			Mongolia		observing		
			Montenegro		observing		
			N. Macedonia	x			
		x	Nepal				
		x	Netherlands	x	participating	x	x
		x	New Zealand		participating	x	
			Nigeria		participating		
			Norway	x	participating	x	
			Pakistan			x	
			Peru		observing		
			Philippines		observing		
		x	Poland	x	observing	x	
		x	Portugal	x	observing	x	
			Romania	x	observing	x	
	x		Russian Fed		participating	x	
	x	x	Saudi Arabia		participating	x	x
			Serbia	x	observing		
		x	Singapore		observing	x	
			Slovakia	x	observing	x	
			Slovenia	x	observing		
	x		South Africa		participating		
			Spain	x	participating	x	x

		x	Sri Lanka		observing		
		x	Sweden	x	participating	x	
		x	Switzerland	x	participating	x	x
			Taiwan			x	x
			Thailand		observing		
			Tunisia		observing		
	x		Turkey	x	observing		x
			Ukraine		observing		
		x	Ukraine			x	
			United Arab Rep			x	
x	x	x	United Kingdom	x	participating	x	x
x	x	x	United States		participating	x	x
		x	Uganda				
		x	Uruguay		observing		
			Zambia				

## Appendix 2 Health Open Standards In Use today

The information for the table below was gathered from from the responses given by 21 countries in the Global Digital Health Initiative White Paper “Connected Health:

Empowering Health Through Interoperability” <sup>30</sup>

Standard	Description	Network/Security Protocols
Digital Imaging and Communications in Medicine (DICOM)	Peer to Peer imaging systems ISO 12052:2017(en)	SOAP/SAML (wrapper). IHE XDS-I Application Level TCP IP
HL7v2	LLP messaging format non xml encoding ANSI/HL7	FTP, SOAP, SMTP
HL7v3	RIM - ISO/HL7 21731 secure text messaging XML encoding	IHE XDS ebXML SOAP/SAML
CDA	XML Document <b>ISO/HL7 27932.</b>	IHE XDS ebXML SOAP/SAML
HL7 FHIR	XML or JSON resource	REST Oauth 2 OpenID Core

<sup>30</sup> [https://s3-ap-southeast-2.amazonaws.com/ehq-production-australia/57f9a51462d5e3f07569d55232fcc11290b99cd6/documents/attachments/000/102/278/original/GDHP\\_Interop\\_2.05.pdf](https://s3-ap-southeast-2.amazonaws.com/ehq-production-australia/57f9a51462d5e3f07569d55232fcc11290b99cd6/documents/attachments/000/102/278/original/GDHP_Interop_2.05.pdf)

## Appendix 3 Standards Mapping

DRAFT

## Appendix 4 Verifiable Credential Myths

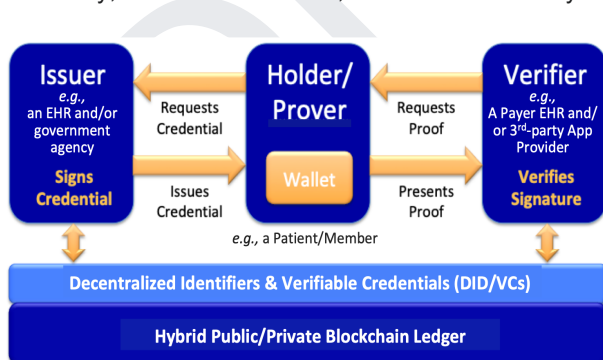
Among the many verifiable credential myths that tend to conflate and confuse, there are four important ones to clarify and demystify.

**Myth #1 verifiable credentials are not analogous nor dependent upon the usage of distributed ledger technology (DLT), or blockchains.**

First, it's important to get a firm grasp of the primary actors in any verifiable credential approach: the top three are the Issuer, the Holder/Prover and the Verifier. These can be combined in a privacy preserving architecture and augmented by a trust and governance model. These three actors are not necessarily dependent upon a blockchain nor any particular centralized or decentralized registry, as verifiable credentials can be issued and verified without it.

That said, for the End-Users to directly receive credentials from the Issuers and directly present them to the Verifiers, a mechanism for the verifier to obtain the public keys controlled by the Issuers is crucial. This could be done by obtaining public keys via a PKI, web pages accessible via HTTPS, or other published and registered locations.

However, as seen in the diagram, these three actors CAN be configured to leverage a blockchain if desired or required. In this scenario a distributed ledger technology (DTL) or “blockchain” is used to meet additional trust requirements like irrefutable audit, provenance, provable privacy and ecosystem governance capabilities. Decentralized Identifiers (DIDs) leveraging a DLT or blockchain is one useful mechanism for key discovery, but as noted above, it is far from the only way to enable key discovery.



Other decentralized implementation techniques have their role to play, but they are neither necessary nor sufficient to achieve a verifiable credentials ecosystem.



## **Myth #2, verifiable credentials are not necessarily equivalent to self-asserted (or self-issued) claims**

The protocols used in verifiable credentials certainly can enable End-Users to present self-asserted or self-issued claims to verifiers. But they can also include verifiable credentials issued by new or existing third party entities (like vendors or digital platforms offering identity services) , or government entities that issue physical identity credentials today (e.g. driving licenses, national IDs). Moreover, verifiable credentials can also be used to convey fine-grained consents, convey a patient's clinical data, or convey other protected resources within the verifiable credential itself. In short, verifiable credentials are much broader, or a "superset" of historical credential types.

Verifiable credentials are not, in and of themselves, equivalent to effective self-sovereignty. Although Verifiable Credentials are often invoked as a means for an End User achieving autonomy and freedom from Issuers and Verifiers, this is hard for verifiable credentials to achieve in real-life use-cases. Two key limitations:

- (1) Even when the Verifier has obtained the claims directly from the End-User, it is still up to the Verifier to decide whether to accept those credentials and provide the service to the End-User (or not).
- (2) Regardless of where the End-User is planning to use a verifiable credential, it is still up to the Issuer to decide whether to issue the credential to the End-User in the first place. Even after the issuance, in most cases, the Issuer retains the right to revoke and invalidate the credential.

Although the terms Verifiable Credential and Self-Sovereign may be conflated and inaccurate based on the reasons above, Verifiable Credentials do offer an important, "privacy preserving" feature. The individual Holder or subject gains control or sovereignty of what claims about herself she chooses to collect and subsequently share; and Issuers remain sovereign on what claims to issue, and the Verifiers remain sovereign on which claims to Rely upon. Thus as it relates to Identity, generally speaking, a "self-sovereign" individual comprises a composite of their own digital identity (or DID) and one or more mutually acceptable verifiable credentials<sup>31</sup> contained in her digital wallet.

## **Myth #3, verifiable credentials are not analogous to use of, nor necessarily compliant with the W3C Verifiable Credentials data model.**

---

<sup>31</sup> In this statement, a verifiable credential could include an ISO 18013-5 mobile driving license, or other government issued credential, configured as a verifiable credential.

Other data models can be used, for example the ISO 18013-5 Mobile Driving License model (where the family of ISO specs includes eID/National IDs, and other government issued credential types). That said, conformance with standard models and protocols are generally necessary to wide scale adoption within a prescribed commercial and/or institutional ecosystem

**Myth #4, verifiable credentials can have varying degrees of openness in terms of participation.**

Some ecosystems, like the ones managed by the governments, health systems, and others, may require certain permissions or certifications for the wallet application providers, credential issuers and verifiers to join their ecosystem, while others may be completely open to anyone to participate. This is just like federated identity management systems today.

## Appendix 5 Other OpenID Foundation Efforts

### OpenID Connect for Identity Assurance

The Identity Assurance specification defines an extension to OpenID Connect [OpenID] for providing identity information, i.e., Verified Claims, along with an explicit statement about the verification status of these Claims (what, how, when, according to what rules, using what evidence). This specification is aimed at enabling use cases requiring strong assurance, for example, to comply with regulatory requirements such as Anti-Money Laundering laws or access to health data, risk mitigation, or fraud prevention.

In such use cases, the Relying Party (RP) needs to understand the trustworthiness or assurance level of the Claims about the End-User that the OpenID Connect Provider (OP) is willing to communicate, along with process-related information and evidence used to verify the End-User Claims. This specification defines a suitable representation and mechanisms the RP will utilize to request Verified Claims about an End-User along with assurance data and for the OP to represent these Verified Claims and accompanying assurance data. For more information see: <https://openid.net/wg/ekyc-ida/>.

### Global Assured Identity Network (GAIN)

In an increasingly interconnected world there is an appetite for global interoperability, whether that is for cross-border payments or the secure transfer of health data. The OI DF is collaborating with a number of organizations to explore this area, including those that have not selected FAPI. In addition, the Foundation is working on the Global Assured Identity Network (GAIN) which has similar aims to support global interoperability for assured identities. It is leveraging several OpenID Foundation standards like OpenID Connect for Identity Assurance, FAPI protocol, and others are in review. The GAIN initiative is currently guided by 5 non-profit entities with a non-binding MOU. The 5 non profits are the International Institute of Finance, the Global Identity Exchange, the Cloud Signature Consortium, the Global Legal Entity Identifier Foundation, and the OpenID Foundation. For more background on the GAIN vision see [gainforum.org](https://gainforum.org), and for more on the GAIN Proof of Concept Community Group, see <https://openid.net/gainpoc/>.

## Appendix 6 Glossary

DRAFT