Design Goals for a Healthcare Identity Environment Architecture

**Version:** 1.0 draft

**Document Date:** 2020-02-dd

**Editors:** Dr. Thomas Sullivan, Martin Smith

**Produced by:** Healthcare Identity Assurance Working Group (HIAWG)

**Status:**

This document is a Group Draft Report produced by the Healthcare Identity Assurance Working Group (HIAWG). See the Kantara Initiative Operating Procedures {op href} for more information.

**Abstract:**

Kantara’s Healthcare Identity Assurance Working Group (HIAWG) is building on the work of the Healthcare Committee of the former Identity Ecosystem Steering Group (IDESG) towards defining design goals (i.e., high-level requirements) for an identity architecture for the healthcare sector. This healthcare-specific architecture should meet the business requirements of that sector so it will be sustainable while also maintaining alignment with the relevant principles from our prior workgroups cited below. We believe these healthcare design goals can be applied globally in appropriate environments.

**PR Option:**

Creative Commons Attribution-Share Alike

**Suggested Citation:**

*Design Goals for a Healthcare Identity Environment Architecture*, Version *1.0*,Kantara Initiative Healthcare Identity Assurance Working Group 2020-03-xx. Kantara Initiative Report. HREF

NOTICE

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third-partyintellectual property rights. This Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review Kantara Initiative’s website (http://www.kantarainitiative.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Directors.



This work is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported License (CC BY‑SA 3.0). To view a copy of the license, visit https://creativecommons.org/licenses/by-sa/3.0/

You are free to:

Share — copy and redistribute the material in any medium or format
Adapt — remix, transform, and build upon the material for any purpose, even commercially.

This license is acceptable for Free Cultural Works.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

Share Alike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

**Notices:**

You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.

No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material.

For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this document.

Copyright: The content of this document is copyright of Kantara Initiative, Inc.
© 2020 Kantara Initiative, Inc.

**Contents**

1. Introduction 4

2. Design Goals for a Healthcare Identity Architecture 5

3. Alignment of HIAWG DeSIGN Goals with NSTIC Principles 7

4. Conclusions 10

5. PROPOSED Follow-ON WOrk 11

5.1 ElaboratE the HIAWG Design Goals 11

5.2 Advance the FIRE WG’s *Distributed Identity Assurance Specification* 11

5.3 Advocate for incorporation of HIAWG Design Goals in healthcare stakeholders’ policies 11

6. Appendix A: Acknowledgements 12

# Introduction

Kantara’s Healthcare Identity Assurance Working Group (HIAWG) is building on the work of the Healthcare Committee of the former NIST supported**,** Identity Ecosystem Steering Group (IDESG) towards defining design goals (i.e., high-level requirements) for an identity architecture for theglobal healthcare sector. This healthcare-specific architecture should meet the business requirements of that sectorso as to insure sustainability. It should also serve as a starting point for online identities being built with a global Healthcare Architecture in mind, along with the ecosystem that supports it. Its provenance includes years of deliberation and substantial alignment with the IDESG’s non-sector-specific Identity Ecosystem Framework (IDEF), which is itself designed to conform to the principles of the 2012 National Strategy for Trusted Identities in Cyberspace (NSTIC.)

The Design Goals below are the IDESG Healthcare Committee design principles as updated by the HIAWG. Table 1, following, maps these HIAWG Design Goals to NSTIC Principles. Two results of this mapping exercise are notable: first, in some cases the WG concluded that a Healthcare Design Goal was not related to any NSTIC Principle, or even negatively related; second, in many cases HIAWG members expressed different interpretations of a Principle, or focused on different aspects of how a particular HIAWG Design Goal might relate to one of the NSTIC Principles. For example, some in the WG interpreted the NSTIC Principle of “Voluntary” as meaning that individuals should have maximum control of their identity information, whereas others, citing the political context in which the NSTIC was created, thought it meant that the Government should not mandate use of the IDEF (or any specific framework) by all relying parties or subscribers (individual users.) The Comments in the mapping table and the HIAWG Member Comments on individual mappings provide some insight into what interpretations and assumptions underlie the alignment scores.

# Design Goals for a Healthcare Identity Architecture

Design goals are high-level requirements for how a system will perform its intended functions. The “system” in this case is an environment comprised of an unspecified number of separately owned and independently managed systems, which include technology (IT) as well as environment-wide rules and standards applicable to all participants. These systems interoperate to provide an identity and access-management (IAM) environment for transactions and information exchanges among healthcare providers and related organizations, their employees and contractors, other stakeholder organizations (e.g. regulators) and individual healthcare customers, that is, patients.

The HIAWG has identified the following as requirements for a healthcare IAM environment:

1. The system shall support the goal of 100% accuracy in identity management and matching of patients to their health records

2. The system shall include "Break the Glass" (BTG) capability for use in emergencies. A BTG capability allows access to information and functions that would not be permitted in non-emergency circumstances. A record of information accessed and actions taken using BTG capability must be included in audit logs (see Requirement 4. below) and notices or receipts should be sent to patients or others affected to inform them of the emergency access.

3. The system shall include features that preserve privacy of identity data, including support for anonymous or pseudonymous access where risk factors allow; use of opaque identifiers; minimum exchange of Personally Identifiable Information (PII) ~~PII~~ a.k.a. Protected Health Information (PHI - in the US Realm) not essential for authentication; and use of claims versus identifying attributes to support authorization.

4. To enable compliance audits and forensics, the system shall create, protect and support analysis of comprehensive logs of access requests, modifications to identity and privileges records, and modifications to the configuration of IAM system components. Integrity of distributed logs also requires time-stamping that is consistent across the environment.

5. All features of the system shall be designed to maximize patient safety and to minimize healthcare providers’ liability arising from inaccurate, duplicate or conflicting identity information.

6. The system shall support flexible, understandable and simple delegation of authority to a “proxy” to access healthcare information and functions. This includes support for simple and inexpensive creation of appropriately strong credentials for the designated proxy (or use of the proxy’s existing credentials that meet applicable standards (see Requirements 7 and 8 below)

7. The system shall support authentication at NIST 800-63-3 AAL1 and AAL2, and federation of authenticators and attributes at FAL1 and FAL2. (Relying Party systems may choose not to accept federated authenticators or attributes.)

8. The system shall support identity proofing of subscribers (holders of acceptable authentication credentials) at appropriate levels of risk mitigation (e.g. At NIST 800-63-3 IAL1 and IAL2 and include a mechanism for IdPs to convey the IAL of a subscriber’s identity securely to Relying Parties.

9. The system shall be resilient, with the ability to sustain critical healthcare operations and to recover quickly in the event of accidental damage, natural disaster or malicious attack.

10. The system shall support effective redress via technological features, contractual agreements, and (if necessary) regulations to assign and enforce liability for intentional identity fraud, negligence, or failure to observe agreed obligations assumed as a participant in the healthcare IAM environment. Liability insurance is recommended in addition or as an alternative to the statuary requirement.

# Alignment of HIAWG DeSIGN Goals with NSTIC Principles

“To “kick start” development of the global architecture we prepared a spreadsheet map or comparison with the US federal sector-initiated Identity design principles in the generic non healthcare space (NSTIC), e.g. all eCommerce.  This spreadsheet helps clearly illustrate the differences  between identity considerations in the healthcare Industry and all other regulated industries, e.g. banking and finance.“

 As indicated by the predominance of green shading in the table below, there is a high degree of alignment between the HIAWG design goals (i.e., high-level business requirements) and the Principles of the National Strategy for Trusted Identities in Cyberspace. The areas of weakest alignment (as indicated by the number of yellow or red cells) are to NSTIC Principles “Voluntary” (table column 2) and “Cost-Effective” (column 6.) As a generalization, areas of non-alignment seem mainly due to the healthcare sector’s relatively stringent requirements for inter-operability and identity security. These requirements in turn add cost to an identity architecture for the sector.

**Table 1.--Mapping of Kantara Health ID Assurance WG (HIAWG) Requirements to NSTIC Principles**

|  | **NSTIC Principle** | **Privacy Enhancing** | **Voluntary** | **Secure** | **Resilient** | **Interoperable** | **Cost Effective** | **Easy to Use** | **Comments** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **HIAWG Design Goal** |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| 100% Accuracy ID Match | A | **Y-1** | **N/A** | **Y - 3** | **Y-3** | **Y-4** | **N-1** | **Y-4** | Zero allowance for ID mismatches = unknown/unlimited cost? |
| "Break the Glass" policy in effect | B | **N-1** | **N-1** | **N/A** | **N/A** | **N/A** | **N/A** | **Y -2** | Access PHI in emergency without express consent |
| Relative Anonymity/Pseudonyms allowed | C | **Y - 5** | **Y - 5** | **N-1** | **N/A** | **N-2** | **N-1** | **Y-3** | Dependent on the Relying Party policies and the nature of the transaction |
| Robust Audit Trails / Precise Time Stamp | D | **Y - 3** | **N-1** | **Y-5** | **Y-1** | **Y - 1** | **N/A** | **Y-2** | Accountability, QA/QI. But easy for whom--Auditor/Security vs. end user provider/patient? |
| Patient Safety/ Liability concerns | E | **Y - 3** | **Y-1** | **Y - 3** | **Y-4** | **N/A** | **Y-1** | **N/A** | Mismatched ID, poor design lead to serious errors and liability |
| Delegate proxy (access) easily  | F | **Y - 2** | **Y-3** | **Y-2** | **Y - 3** | **N/A** | **N/A** | **Y-5** | Consistent with longstanding HIPAA rights |
| Strong MFA to enhance security | G | **Y-3** | **N/A** | **Y - 5** | **Y-2** | **Y-4** | **Y-2** | **N-1** | MFA = Multi-factor Authentication |
| Standards-based risk-appropriate identity proofing | H | **Y-1** | **N-1** | **Y-5** | **N/A** | **Y-3** | **N-2** | **N-2** |  See H1-7 in comments below |
| Resilience | I | **Y-4** | **N/A** | **Y-3** | **Y-5** | **Y-2** | **Y-2** | **Y-4** | The ability “to recover and adapt to drastic and abrupt change”  |
| Legal Redress allowed/defined | J | **Y - 5** | **Y - 2** | **Y-2** | **Y-2** | **Y-3** | **Y - 2** | **Y-1** | To counter intentional online ID fraud/abuse |

**Key to cell scores:**

Y = HIAWG Requirement consistent with or supports NSTIC principle

N= HIAWG requirement inconsistent with or does not support NSTIC principle

N/A = HIAWG requirement doesn’t map to any NSTIC principle or relationship is ambiguous

Numeric scores 1-5: strength of positive or negative relationship. 1 = weakest, 5 = strongest

**Interpreting the matrix—Examples:**

Score of **Y-5** in cell D3 means that **Robust Audit Trails** (HIAWG requirement D) are judged to be **strongly supportive** of **Security** (NSTIC Principle 3)

Score of **N-1** in cell G7 means that **Strong MFA** (HIAWG requirement G) are judged to be **weakly inconsistent** with **Easy to Use** (NSTIC Principle 7)

**HIAWG Member Comments on Individual Cell Scores**

|  |  |
| --- | --- |
| **Cell** | **Comment** |
| A-1 | Marginal extra protection against inadvertent disclosure of ID or medical info. |
| A-3 | Cyber-attack on IDs scored under HIAWG G (MFA). This positive score is for fewer inadvertent errors |
| A-6 | Generally, achieving 100% reliability of anything is very costly |
| B-1 | Only minor negative impact from no prior consent for access, especially with accountability for BTG access provided by audit |
| B-2 | Very minor compromise of consent especially if consent is granted in advance for unspecified emergency situations |
| B-7 | Good BTG implementation provides clear, quick path for appropriate emergency response |
| C-2 | Score based on interpreting NSTIC "Voluntary" principle as "providing maximizing user control" (not the original meaning, which was related to concern about Government-mandated “national IDs”) |
| C-3 | Providing relative anonymity may inhibit some authorized forensics but technology is available to implement with reasonable limitations |
| C-5 | Adds a requirement (meaning more complexity) for all participants considering supporting federated credentials |
| C-6 | Adds cost to implement for all federating participants |
| D-1 | Provides accountability that will inhibit unauthorized info access (e.g. "browsing”) |
| D-2 | Compromises anonymity, but technical and policy controls can assure any compromise is limited and accountable  |
| D-4 | Not the main resource for restoring data after a disaster or compromise but might contribute in some cases |
| D-5 | Small positive score for precise timestamping |
| F-6 | Resilient systems are costly to implement and operate, but likely less costly than down-time of increasingly essential IT systems  |
| H-1 | Positive score based on better protection of sensitive information.  |
| H-5 | Well-defined standards-based proofing is essential for acceptance of federated ID credentials.  |
| H-6 | Meaningful ID proofing is more expensive than current “known-to-the-practice” process |
| H-7 | Meaningful risk-appropriate ID proofing will likely make initial credential issuance a longer and more complicated process for user/subscribers – especially for healthcare-provider staff |
| J-5 | Effective redress procedures provide the basis for “trust” relationships among participants in a federated environment |

# Conclusions

As indicated above, there appears to be generally good alignment between the HIAWG Design Goals (i.e., high-level business requirements) and the Principles of the National Strategy for Trusted Identities in Cyberspace. However, the Design Goals are very far from being sufficiently detailed to serve as requirements for an implementable architecture, and as detail is added there will certainly be trade-offs to be made. For example, it seems likely that requirements for security, which significantly depend on accountability of users for their actions, will limit the extent to which user activity can be anonymous. In the healthcare sector particularly, current US Federal policymakers seem inclined to rely on regulation to achieve one NSTIC Principle (interoperability), seemingly at the expense of another Principle (voluntary.) To progress toward an implementable healthcare identity architecture these apparent inconsistencies (or at least trade-offs) will have to be confronted and resolved.

# PROPOSED Follow-ON WOrk

As stated in its Charter, the HIAWG's *“primary focus is to adapt the [NSTIC-Principles-based] IDEF framework to the specific requirements and use-cases of the healthcare sector, and to encourage adoption of this profile of the IDEF throughout the healthcare community.”* To be useful, this profile—characterized in this Report as a *Healthcare Identity Environment Architecture*—should be sufficiently specified that it is implementable, ideally with a choice of commercial or open-source technology solutions. It should also of course satisfy the operational requirements of healthcare delivery while taking into account the perspectives of healthcare providers, consumers and regulators. The Working Group has identified three follow-on initiatives to progress toward an implementable architecture.

## 5.1 ElaboratE the HIAWG Design Goals

The WG is considering how to take the very high-level Design Goals to the next level of specificity, and is examining the possibility of leveraging for this purpose an existing document, *Important Considerations When Planning a National Healthcare Identifier,* which has been contributed by HIAWG participant Barry Hieb, M.D., of Global Patient Identifiers, Inc.

## 5.2 Advance the FIRE WG’s *Distributed Identity Assurance Specification*

The WG is collaborating with the FIRE WG on their specification, currently a WG-approved draft, for authentication credentials with specific reference to a use-case based on patient access to multiple healthcare providers participating in a trusted on-line environment. This specification addresses a capability gap in the provision and use of portable, reusable patient authentication credentials.

## 5.3 Advocate for incorporation of HIAWG Design Goals in healthcare stakeholders’ policies

The WG will continue to be active in promoting awareness of the Design Principles and for their incorporation in US Federal policy and program planning. This advocacy is conducted through participation on conferences and in meetings with US healthcare sector policymakers and influencers.

# Appendix A: Acknowledgements

The authors gratefully acknowledge the contributions of the participants of the Healthcare Identity Assurance Working Group, the list of whom can be found in the WG Participant Roster. We especially thank these active contributors:

* Brian Ahier
* Ken Dagg
* Barry Hieb
* Jim Kragh
* Tom Jones
* Catherine Schulten
* Colin Wallis