

Comments on Federal Health IT Strategic Plan

**To: Dr. Don Rucker, Office of the National Coordinator**

**Date:** 2020-02-04

**From Kantara Working Groups**:

1. Health Identity Assurance – Chair Thomas Sullivan M. D.
2. Federated Identifiers – Chair Jim Kragh

This submission supports the immediate release of the Interoperability and Patient Access rules of the 21st Century Cures Act that dates back to 1994 when Dr Bill Braithwaite initiated the path to HIPAA and worked with HHS in promoting keep this text. In 2015 HIMSS formed the Identity Management Task Force that Dr Braithwaite chaired (the signatories to this submission were active contributors) underscoring the importance of having a trusted digital identity and patient data portability. As a personal friend and collogue of the signatories, Dr Bill, knowing his patient centric values, was contacted and he shared the following:

The federal government establish standards for the private and secure exchange of electronic health information in 1994 with the creation of the Administrative Simplification Subtitle which passed into law as part of HIPAA in 1996.  This effort has evolved through issuance of federal regulations to the implementation of HIPAA and subsequent laws that were passed to stiffen requirements and penalties that the US Congress perceived appropriate for our industry. EHR vendors resisted any attempt to implement a standardized information exchange.  Each institution implemented proprietary, partial solutions that restricted and blocked the efficient implementation of a private and secure health information highway that all could access. Ms. Faulkner’s position is like other vendors who belive they have solved the prolems. However, interoperability only works if everyone buys and implements exactly the same software suite from a single vendor. But the vendor systems are NOT the same, hence not interoperable because each system is implemented in a different way with different access protocols with no standardized process for capturing and sharing clinical data and PHI. Hence, vendors capture and store PHI in their system silos for monetization.

**The balance of this submission addresses issues for inclusion in the 2020-2025 iteration of the Federal Health IT Strategic Plan which we fully support.**

Thomas Sullivan Jim Kragh

Thomas Sullivan M. D., Chair Jim Kragh, Chair

Healthcare Identity Assurance Work Group Federated Identifiers Work Group

# Comments

**Comments to the 2020-2025 Federal Health IT Strategic Plan to address the issues:**

**These comment are also submitted to the** [**website**](https://www.healthit.gov/topic/2020-2025-federal-health-it-strategic-plan)**.**

1. Privacy risks are increased by interoperability: Solution: Ensure that all software whether in the cloud or in the patient’s smartphone is known to accept responsibility for patient choice and privacy protection.
2. Patient Privacy can only be protected if all computer hardware and software is known to be secure. Solution: some means to assuring the patient’s device and app must exist alongside the existing controls for the web site security.
3. All patients must be able to know that the web sites they visit are fully compliant with HIPAA requirements without cost before they share sensitive data. Solution: a trust registry accessible by user apps must be freely available on the web.
4. Patients must be able to know what data they are asking one EHR to share with other providers. Solution a common taxonomy of mediacal data categories for user consent is required. The list must be short and understood by 90% of patients.
5. Patients can download and share their health information. Soluiton: Smartphone apps are assessed and entered into a US healthcare assurance registery that is shared with existing EHR web sites.
6. Vendors selling smart phone apps have a very poor record of protecting user data (see section on patient choice below) Solution: [Kantara Initiative First to Market with NIST SP 800-63-3 Third Party Assessment, Approval and Trust Mark](https://kantarainitiative.org/kantara-initiative-first-to-market-with-nist-sp-800-63-3-third-party-assessment-approval-and-trust-mark/) can serve as a paradigm for a US Healthcare program to assess smartphone apps to protect user privacy.
7. An EHR platform is interoperable within that vendors’ health systems’ enterprise. However, interoperability only works if everyone buys and implements exactly the same software suite from a single vendor. But EHR systems are NOT the same, hence not interoperable because each system is implemented in a different way with different access protocols with no standardized process for capturing and sharing clinical data and PHI Solution: Interoperability testing and clinical data standardization will be part of all software assessements..

Documents for consideration:, Design Principles for a Healthcare Identity Environment (section 2 following) Patient Choice (section 3 following) and [Distributed Identity Assurance Specification (latest version available online.)](https://kantarainitiative.org/confluence/display/WT/Draft+Recommendations)

**Anyone can Direct Comments on any of these documents to:** <https://github.com/KantaraInitiative/DistributedAssurance/issues>

# Principles of Identity Assurance

## Introduction

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, supported by NIST) towards defining design principles/goals (i.e., high-level requirements) for an identity architecture for the national healthcare sector. This healthcare-specific architecture should meet the business requirements of that sector while also maintaining 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 Principles/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 Principles/Goals for a Healthcare Identity Environment Architecture

Design princiles/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 PII 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 NIST 800-63-3 IAL1 and IAL2, and include a mechanism 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.**

**Table 1.--Mapping of Kantara Health ID Assurance WG (HIAWG) Requirements against 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/A = HIAWG requirement doesn’t map to any NSTIC principle or relationship is ambiguous

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

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. e.g. NIST 800-63-3 or later or prevailing standards Should there be a private sector equivalent, simpler to understand and implement? Kantara could possibly help in this area. |
| 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 |

# Patient choice

The options that a patient should have in accessing and sharing their [Protected Health Information (PHI)](https://tcwiki.azurewebsites.net/index.php?title=PHI) with trusted medical providers.

## Source

The Federated Identifiers for Resilient Ecosystems Work Group of the Kantara Initiative.

## Context

* The major context for this page is an environment where user's private data is treated like a commodity to be bought and sold. These two postings in the Sunday New York Times on 2020-01-26 demonstrate conclusively that a [Trustworthy Healthcare Ecosystem](https://wiki.idesg.org/wiki/index.php/Trustworthy_Healthcare_Ecosystem) requires more attention to the handling of healthcare data that is common at this time:
  + The report on **The Secretive Company That Might End Privacy as we Know it** received more reader attention than any reports on the Impeachment trial of the President or even the tribulations of the Duke and Duchess of Sussex.
  + An entire section of the paper **"One Nation, Tracked"** describing **"The Smartphone Data Collection Industry"** showed conclusively that we cannot trust the phone apps that brought us to this point.
* This pattern is a sub-set of the [User Choice Pattern](https://wiki.idesg.org/wiki/index.php/User_Choice_Pattern) which covers the general user choice issues. It contains the general context and should be read in conjunction with this page.
* This document assumes that the \*[Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2](https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf) (2019-04-19) will apply. From that it assumes that some means must be found for level 2 authentication of patients that will not be faced with the same rejection as was evidenced in earlier attempts at TLS client authentication.
* Patient choice is acclaimed by existing health care solutions, often as a means for the providers to avoid the responsibility for making good, but tough, clinical and security decisions which might possibly result in bad outcomes and liability to large tort actions. If the blame can be placed on the patient, the care provider might avoid lawsuits.
* For a long time, **actual** patient choice has been ignored. Now that more enterprises have found that patients will not use products that they don't like or don't trust, every enterprise is claiming that their applications preserve patient choice. The reality does not quite live up to their claims.
* To understand what applications will satisfy patients, we cannot rely on enterprises that peddle solutions, we need to give the patients information about their choices and only then ask the patients what is really important to them.

The term "enterprise" is used in this document to include all purveyors of health care solutions from governments and non-profits to profit making companies.

## Problems

* Patients have all expressed a desire to control what and where they share their [Protected Health Information (PHI)](https://tcwiki.azurewebsites.net/index.php?title=PHI).
* Patients also ask to have control of the applications that run on their smartphones particularly with respect to the way that they handle user private information and the way that they intrude on the attention of the user.
* If the patient chooses an application for their smartphone that downloads PHI, then that application has complete control over where that data goes.
* If the healthcare community decides to allow any smartphone application that the patient chooses to install on the smartphone, then the patient is at risk to lose control of their PHI.
* If the patient chooses to upload their PHI to just any web site without knowledge of that sites' controls, then the patient is at risk to lose control of their PHI.
* Without some other trust mark on the app, it is very difficult for the patient to determine if the app is covered by HIPAA. "If you see the term 'we are HIPAA-compliant', the basic rule of thumb is the program does not fall under HIPAA" from Pam Dixon, executive director of the World Privacy Forum as quoted by Thorin Klosowski in "Consider the Consequences of Trading Your Health Data. (2020-02-03) New York Times p. B7.
* The patient must be given the tools to assure that their PHI remains under their control. The healthcare community will lose the patient's trust if they don't enforce that.
* The biggest problem for the covered HIPAA entity is what level of assurance of patient intent do they require to:

1. Release data to the user, especially in machine readable form.
2. Accept data input from the user to be added to the patient's permanent EHR.
3. Accept medical directives from the patient, especially POLST directives.

* As a recipient of HIPAA covered data, any patient-centric health care app MUST take responsibility for protecting the data.
* Electronic Health Record sites must assure that any patient app accepts this responsibility before sending them PHI.
* All computer application software that is running on internet connected computers is subject to a daily barrage of attacks trying to exploit vulnerabilities in that software or the gullibility of the people operating those computers. The [Healthcare IT News reported](https://www.healthcareitnews.com/news/8-out-10-mobile-health-apps-open-hipaa-violations-hacking-data-theft) that: "8 out of 10 mobile health apps open to HIPAA violations, hacking, data theft. Though the majority of executives surveyed by Arxan said they believe their apps are secure."
* A [recent evaluation of the security of health apps on smartphones](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6371412/) revealed the following: "We identified 116 eligible mobile phone apps. Of those, 4% (5/116) received a transparency score of acceptable, 28% (32/116) questionable, and 68% (79/116) unacceptable. Only a minority of the apps (49%) had a privacy policy." Clearly leaving security up to app developers without verification is not working today.

## Solutions

* The computer industry has learned that security cannot be a choice and has taken the responsibility to assure that their software does not expose the user to exploits that are launched regularly from any site that has access to the internet.
* If the patient is to have a choice about the release of their protected health information (PHI), they must be able to rely on the software that is installed on the healthcare provider’s computers as well as any software that they use on their own computers.
* To enable real patient choice, the healthcare community must create a trust registry of web sites and applications that are to be trusted with patient healthcare information (covered HIPAA entities). In other words, enabling patient choice on access to their data, the patient must be limited to the use of secure sites and applications that can be trusted to maintain the security of that information.
* The healthcare community must prevent any sites or apps that are not in the US Healthcare Assurance Registry from downloading patient data.
* The healthcare community should prevent any user app from uploading data is not from a trusted site or app into the patient's EHR.
* To be sure that patient concerns are met, a [Trustworthy Healthcare Ecosystem](https://wiki.idesg.org/wiki/index.php/Trustworthy_Healthcare_Ecosystem) must exist to be able to strongly identify these actors:

1. The Patient must be able to prove that they are the owner (or [Guardian](https://wiki.idesg.org/wiki/index.php/Guardian) of the owner) of the PHI.
2. The Patient app must be trusted to faithfully present the patient authentication and protect PHI that the patient downloads.
3. The source of the data must be trusted to show the provenance of the data. That is to show that the data is legitimate and accurate.
4. If the patient chooses to share PHI, they must be able to assure that the recipient of the data will treat the data with the full protections of HIPAA.

* The question about PHI that is released to non-HIPAA covered entities has not yet been addressed. But is it clear that the patient needs to understand the implications and risks of such a release before it happens.

1. **Other functionality that a device app could supply**
2. The app could be used by a medical record source to determine which categories of medical records the patient wants to share with other HIPAA covered entities.
3. The app could respond to requests by an EHR for current information, with the data held by the user, or by forwarding the request to the source EHR.
4. The patient or legal system can enable guardians to use the app for access or update of patient data.

## Reference Material

The following use cases contain details about the location where a user agent maintains Patient Choice (i.e. on the user's smartphone or in the cloud) among other issues in a [Trustworthy Healthcare Ecosystem](https://wiki.idesg.org/wiki/index.php/Trustworthy_Healthcare_Ecosystem).

* The [Remote Attestation Use Case](https://wiki.idesg.org/wiki/index.php/Remote_Attestation_Use_Case) wiki page describes a user with a Smartphone going through a series of actions that will provide subsequent statements from that user on that phone with a higher level of assurance.
* The [User Agent in the Cloud](https://wiki.idesg.org/wiki/index.php/User_Agent_in_the_Cloud) wiki page describes a user with a modern browser on a internet connected computing device establishing an agent on a trustworthy website to allow access to information on their behalf.

These patient choices and their attendant liability are addressed in Design Principles/Goals for a Healthcare Identity Environment Architecture above, a current copy will be maintained on [the Kantara website](https://kantarainitiative.org/confluence/display/healthidassurance/Identity+Assurance+Principles).