**From the Kantara Health Identity Assurance Workgroup (HIAWG)**

[**Identity Assurance Principles**](https://kantarainitiative.org/confluence/display/healthidassurance/File+Lists?preview=/72581926/129566264/NIST%20and%20MITRE%20identity%20proofing%20analysis%20v%202020-06-26.docx)

**The working group has identified the following as requirements for a healthcare identity ecosystem (shortened for clarity):**

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 record of information accessed, and actions taken using BTG capability must be included in audit logs 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 pseudonymous access where risk factors allow.
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 identity ecosystem components.
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.
7. The system shall support authentication at NIST 800-63-3 (and its successors), AAL1 and AAL2, and federation of authenticators and attributes at FAL1 and FAL2 and its successors.
8. The system shall support identity proofing of subscribers at NIST 800-63-3 IAL1 and IAL2 and include a mechanism to convey the level 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 regulations to assign and enforce liability for intentional identity fraud, negligence, or failure to observe agreed obligations assumed as a participant in the healthcare identity ecosystem.