Patient Identifier Requirements v.17 11/8/15

IDESG Healthcare committee

Patient (human) Identifier Requirements

1. **Abstract –** Nothing in the identifier should either require or depend on specific properties of either the associated individual or the type of information associated with the identifier
2. **Capacity/scalability –** The identifier must be capable of covering the associated population for an indefinite number of years
3. **Compact –** The identifier should be as terse as possible.
4. **Usable, Deployable and Flexible –** The identifier must be readily processed in both manual and automated systems. It must be of a form that can be deployed across a variety of media including but not limited to cell phones, mobile apps, bar codes, smart chips, printed forms and magnetic strips**.**
5. **Globally unique** – Each identifier must be guaranteed unique when it is issued.
6. **Language independent –** Nothing in the identifier should represent a dependence on a specific language.
7. **Standards-based –** The use of a standard enables maximum adoption by avoiding competitive issues that arise if a proprietary solution is established.
8. **Unambiguous –** The printed representation of the identifier should not contain unclear entities such as the ability to confuse the letter o with the digit 0.
9. **Uniform syntax –** Each identifier should conform to the same syntax specifications.

Patient (human) Identifier System Requirements

1. **100% accurate** – Proper use of the system should enable 100% accurate identification for 100% of the participants.
2. **Anonymous use –** An identifier should be able to be used to represent an anonymous or pseudonymous individual. Identifiers can be used for both identifiable and non-identifiable purposes. Also, a system function that uses "blinding" is one method to render re-identification less likely.
3. **Authentication capable** – It must be possible to augment the identification system with a variety of authentication techniques such as biometrics and knowledge based authentication (KBA).
4. **Break the glass –** It should be possible to override anonymous operation of an identifier for specified situations (such as medical emergencies or law enforcement) and to restore anonymity when that situation has been resolved.
5. **Compatible with existing IT** – To the extent possible the identifier system should build on existing IT capabilities rather than forcing them to be replaced.
6. **Continuous availability** – The identification system should be available on a 24 * 7 basis.
7. **Cost effective –** The identifier system should be designed to be as inexpensive as possible while providing the maximum value feasible.
8. **Efficiency –** All identifier operations should function efficiently despite the complex distributed environment where the identifiers are used.

9. **Resilient and Error tolerant –** Resilience is a term that means the identity can be recovered and re-established even after theft or compromise. In any complex system mistakes will happen. Replacement of an identifier to correct an error situation should be rapid, easy, and supported across the network. A thief should not be able to create valid identifiers. Techniques such as encryption must be used to offer the maximum security possible. See also #10.
10. **Verifiable –** The recipient and all users of an identifier can verify that it is valid. This can be assisted though the use of several methods, including internal mistyping checks, database lookups, multifactor authentication (MFA) and others. Using an internal error detection or correction scheme (could be as simple as a check digit) makes sense for identifiers that might be manually transcribed (like Medical Record Numbers - MRNs), but the algorithm must be widely known and implemented. This requirement is closely related to #9.
11. **Decentralized operation –** The identification system must be sufficiently distributed to ensure that it is not susceptible to single point of failure incidents.
12. **Data location –** The identifier system may track the 'locations' where each identifier has been used. This requirement should be optional, e.g. the "right to be forgotten" as is being discussed in Europe.
13. **Future proof –** To the extent possible the identification system must be able to adapt gracefully to new functions and new requirements that were not foreseen at the time the system was created.
14. **Language independent** – The identification system should be deployable across all languages.
15. **Incremental –** To the extent possible the identifier system should be additive to existing IT systems rather than replacing them.
16. **Minimal personal information –** The operation of the identification system must be designed to keep to a minimum the amount of personal information required for correct operation.
17. **Multiple identifiers –** There may be circumstances which justify the issuance of multiple identifiers to an individual.
18. **Network-based operation –** Identifiers will be used across an arbitrary variety of distributed locations. Identifier activities (creation, tracking, management, etc.) must function properly in this distributed environment.
19. **Non-repudiation** – Significant identification and authentication actions must be recorded in a manner that cannot be refuted.
20. **Permanent and Unique –** No human identifier is ever reused. The system must provide a "functionally unlimited" number of identifiers to ensure that reuse is not required. With the exception of dealing with error, theft situations or patient choice, it should not be necessary for an identifier to be invalidated. The identification system should intentionally avoid capabilities that might lead to the reuse of identifiers.
21. **Person empowering –** The identification system should maximize individual choice rather than imposing top-down restrictions.
22. **Privacy enhancing –** Use of the identifier system for humans must be under the control of the involved individual and should enhance rather than degrade that person's privacy. The system should have the capacity to be able to provide concurrent support for a variety of different privacy paradigms, including adding extensions to address basic privacy and security constraints.
23. **Progressive deployment –** The identifier system must be able to deliver value even when only part of the target population has received identifiers. It should not be necessary for the

identifier to be fully deployed throughout a population in order to gain benefit from the system.

24. **Readily deployable** – The technologies used in the identification system should be readily available, inexpensive, easily understood and reliable.
25. **Real-time operation** – New identifiers can be issued whenever needed and in a matter of seconds.
26. **Simplicity –** The identifier system and its operation should be as easy as possible to understand and to use.
27. **Termination –** There must be an invalidation mechanism which permits any identifier to be rapidly and permanently deactivated.
28. **Time-stamping** – The identification system must keep track of the date and time when significant identification events occur.
29. **Universal** – Any person with a valid need should be able to receive an identifier.
30. **Voluntary and mandatory deployment** –identifiers should be deployable in both voluntary (each individual decides whether to receive an identifier) and mandatory (each individual is issued an identifier) modes.

Additional Comments

- "Known to the practice" (healthcare) – Proper use of an identifier means it is stored in the local organization's EMPI system. When a person presents an ID that is documented in the local EMPI then that person is by definition "known to the practice." If the ID is not present in the EMPI then that person is not known to the practice.
- Patient safety (healthcare) – Privacy in healthcare may be achieved through the use of multiple identifiers by an individual to segment their medical information. However, for such individuals patient safety must be enabled through the use of clinical decision support which has visibility to all of the identifiers being used by that individual. An alert system should draw attention to the existence of multiple identifiers for one individual as part of a safety protocol.
- Maximize local operation – A properly implemented identity system will enable most operations to be accomplished through interactions at the local level. Nevertheless, the system will need the capacity to access audited, centralized identity services.
- Anonymous patient matching – Patients may choose to be anonymous in order to keep some of their sensitive associated information private. Alternatively, organizations may choose to anonymize data for reporting purposes such as public health, research, education and the like. Some members of our IDESG Healthcare committee are collaborating with selected HIMSS Identity management workgroups related to anonymity, pseudonomy, proxy access and patient identity integrity.
- **Cyberphysical Devices and Identity:** Identifiers for inanimate and non-human entities, objects and interfaces addressing medical devices (Cyberphysical devices) and the Internet of Things (IOT) are being addressed by the FDA and NIST. [**Supplemental guidance** listed below will specifically but briefly address this issue. Other entities are researching this also, especially NCCOE and HEART.]

Supplemental Guidance:

The Internet of Things (IOT) or Cyberphysical Devices (as it relates to the medical field), can include biomedical devices, medical devices and implants. Most of these include hardware, software and networks to operate, nearly all in wireless (remote medicine or ambulatory) environments. It is well documented that there are numerous "adverse patient events" and "hacking" of medical devices, threatening the safety, health and lives of people.

The identity of these devices are central to their safe operation and a higher security is needed, at least LOA3. There must be a mechanism whereby a person and their device must match with a geolocation. In addition, sensor data must be accurate, alerts must be accurate, and responses (actions) must be accurate.

The operation of these devices requires higher levels of authentication by persons authorized to access these "endpoints". Special consideration should be given to the automation protocols of network attached medical devices, most of these operating on cell phone networks. Accurate clockwork, meaning syncing with the latest NIST atomic clocks and digital time stamping is recommended.

A digital medical device must utilize a globally unique identifier and all transmissions be protected with strong encryption, digital signatures and mutual authentication between endpoints. An understanding of workflow for authenticating to a device at LOA3 is required. There is a fundamental difference between addresses and identifier of devices. There is also a fundamental difference between digital devices and analog/optical functionality. All vectors of attack need to be considered.

http://www.nist.gov/el/nist-releases-draft-framework-cyber-physical-systems-developers.cfm