Appendix 1: Identity Management Maturity Model

A client registry is foundational to improving health outcomes, lowering costs, and increasing efficiency. We propose a maturity model for identity management based on existing maturity models. Table 1, Identity Management Maturity Model, illustrates the move from the siloed and peer-to-peer maturity level to the interoperable maturity levels with regard to the value-add for public health, the added capabilities and accountabilities. The maturity model frames the user stories for feature development.

The maturity levels[1] are based on the ability to share information and associated responsibilities for governance:

- **Siloed systems** are isolated implementations where there is little to no sharing of information. This is common in low-resources settings where many projects have historically created systems for their use case without coordination. The lack of information exchange makes them inefficient in both the clinical sense and with regard to business allocations. There is more potential for errors and lost opportunities for holistic clinical care. An example of siloed systems are multiple EMRs that are not connected to one another.
- **Peer-to-peer (integrated) systems** are a common solution to increase the business value-add of peer-to-peer systems. Often this means custom systems integration but without standards. While the solutions may perform their roles, the exchange of information is tightly coupled (integration not interoperability). Peer-to-peer systems are difficult to scale to other systems as they are custom solutions. An example of peer-to-peer (integration) is when an EMR is connected to a lab diagnosis system.
- **Interoperable systems** employ standards-based exchanges. Solutions based on them, like shared health records, solve double-counting. This maturity level has the least potential for clinical errors. However, by being the most flexible and powerful, this maturity level requires the highest responsibility for governance, IT security, and privacy. This means managing a broad spectrum of trust levels with participating systems.

Across the maturity model, there are critical implications for clinical care and other health outcomes for different actors:

- For patient and registration actors, the demographic patient information is updated at the point-of-care (POC). This results in duplicate and out-of-date patient demographic information. At the interoperable maturity level the demographic information may be linked to other records of the same patient information and may be distributed to other systems (if it's the source of truth or golden record).
- For clinicians at the siloed maturity level, they may only view patient demographic and clinical information in their system, and those that they are peering with if at the peer-to-peer level. But with a unique identifier and a separate process to create a shared health record, the clinician has the possibility to view the continuity of care of participating systems and thus the patient may receive more holistic care with less possibility for error as clinicians have more information about patient needs.
- Point-of-care (POC) system administrators assign their own identifiers. This fragmentation is overcome with record linkage at the interoperable maturity level. Any source ID designations are accepted and unaltered in the Client Registry, but they are also linked by the Client Registry to a unique identifier which links back to the originating system. This allows maximum flexibility and security where source data systems may not be trusted, so they may only update fields in their own records but still participate in the system and use unique identifiers provided by the Client Registry.
- Contact tracers in the siloed and peer-to-peer maturity models rely on information that may be different at each POC, while at the interoperable maturity level they may use linked records to use alternative addresses.
- At the interoperable maturity level and with shared health record, case-based surveillance officers may eliminate double-counting and create time-series (longitudinal) analysis to support

[1] The maturity levels are adapted from the Federated Vision for a Facility Registry, Digital Square.

surveillance from at any level of granularity, from the patient-level and up to administrative and international boundaries.

- Similarly, at the interoperable maturity level and with a shared health record, reporting actors may eliminate double-counting in reporting, and may be more agile in their timeliness and responsiveness to shifting reporting requirements; indicators can be aggregated up from any level and cross-tabulated on the fly through attributes like age, gender, and condition.
- At the interoperable maturity level, there are substantial requirements for and capacities with regard to governance. Management actors must be able to audit and tune the system along the full spectrum of levels of trust for systems, nodes, and users. With attention to best practices in health information systems only the absolute necessary data may be shared or linked, under a rigid governance process to ensure privacy.

Table 1: Maturity Model for Identity Management

Business Roles (Actors)	**Maturity Level**		
	Siloed: Isolated, inefficient, more potential for errors and lost opportunities for holistic clinica care. Difficult to share health information. Low levels of governance.	**Peer-to-peer (Integrated)**: Greater data sharing through custom systems integration but without standards. Difficult to scale to other systems. Some governance.	**Interoperable**: Standards-based exchange. Less double-counting. Least potential for clinical errors. Most flexible and powerful. Highest responsibility for governance.
Patient	Provides demographic information to Registration Clerk but has no view of his/her/their own data. Depending on the siloed system, the patient may have access to their data.	Provides demographic information to Registration Clerk but has no view of his/her/their own data. Depending on the siloed system, the patient may have access to their data.	Provides demographic information to the Registration Clerk; updated demographic information is stored and potentially available as clinical information stored in a SHR.
Registration Clerk	Updates information at each point-of-care.	Updates information at each point-of-care.	Updates information at each point-of-care and those records are linked together by the Client Registry.
Clinician	May view patient data in the clinical EMR. Data may be captured on paper and entered into EMR at the end of the day or week for reporting purposes. Diagnoses are often added using a manual process.	Only views patient data captured by the clinical EMR or other system. Diagnoses may be electronically added.	Record linkages can be used in a separate process to create a shared health record. The clinician has the possibility to view a patient's health history through access to a shared health record created by participating systems.
Point of Care (POC) system administrator	Assigns local system IDs based on functionality of the local system, absent coordination.	Assigns IDs based on functionality of the local system, absent coordination.	Any ID designations accepted as records are designated with their source ID, while source records are also linked through a Client Registry Unique ID (CRUID) within the client registry.
Community contact tracer	Uses information limited to that captured in local POC to trace patients.	Uses information limited to that captured in local POC to trace patients.	Uses additional patient data stored in linked records, such as alternative addresses, to enhance patient tracing.

Case-based surveillance officer	POS may assist in identifying cases to report, but reporting will be manual	POS may assist in identifying cases to report, but reporting can be manual or electronic.	Provides a foundation for duplicate reporting to be addressed.
M&E Specialist	Aggregates indicators and metrics for their system. Often manual process or done in Excel.	Aggregates indicators and metrics for their system. Often manual process or done in Excel.	Provides a foundation for duplicate counting to be addressed.
System and governance owners	Limited view into siloes. Governance of confidentiality and privacy is not auditable except in-person at each POC.	Limited view into siloes. Governance of confidentiality and privacy is not auditable except in-person at each POC.	Greatest responsibility for managing confidentiality, privacy, and IT security. Must manage the full spectrum of levels of trust for systems, nodes, and users.