Table of Contents

Backgrounder: eCQM Components

In August 2016, ONC convened a SIM Technical Assistance event where participating state teams could assess their current infrastructure using a schematic that presented the components as a related "stack," with certain components being foundational.

It is not necessary for the Connecticut eCQM Design Group to make decisions about several of the components, but it is important to have a working understanding of all components to understand how they relate to each other, and how they can support the desired functionality for the eventual eCQM solution.

Key Components to Consider Described in 3/14/2017 Presentation

Foundational Components

Organizational Governance (Accountability, Oversight, & Rules of Engagement)

Governance for an eCQM solution refers to a multi-stakeholder framework, which may include state, federal, and private entities to manage information throughout its lifecycle. The governance framework ensures a collective approach to strategy, operations, and managing requirements (regulatory, legal, risk, and environmental). Whether undertaken by a market, a network or through formal or informal organizations, it is important to craft a consistent approach to laws, norms, power, or language, accountability, oversight, and rules of engagement for all the processes of governing the eCQM solution.

Examples: enabling legislation; empowered advisory councils; senior executive authority; multi-payer collaborative.

Note: State government has a unique governing role that is separate from and in addition to the framework discussed above. This is separate from national governance activities, such as CareQuality and Commonwell.

Policy & Legal

Policy and legal parameters that apply to everyone involved in the eCQM solution may include health IT policy levers, which are defined as any form of incentive, penalty, or mandate used to effectuate change in support of health IT adoption, use, or interoperability.

State level policy may include state laws, state regulations, state funding, and state programs (including Medicaid activities and health care programs beyond Medicaid) that direct the spending of state money to advance and sustain technical investments, ensure secure exchange and use of health information, and establish required criteria for technology infrastructure.

Examples: legislation; regulations authorized by legislation; medical board policies; Medicaid policies; policies for program implementation; creation of data use agreements; vendor agreements, etc.

Data Use Agreements

Data Use Agreements (DUAs) are contractual documents used for the transfer of health care data, which is subject to restrictions on its use and disclosure. DUAs serve to outline the terms and conditions of the transfer. Specifically, DUAs address important issues such as limitations on use of the data, obligations to safeguard the data, liability for harm arising from the use of the data, publication, and privacy rights that are associated with transfers of confidential or protected data. The understanding established by a DUA can help avoid later issues by clearly setting forth the expectations of the parties (provider and recipient).[1]

[1] http://research.unc.edu/files/2013/04/CCM3_039360.pdf

Because different stakeholders may share different levels of detail in their data sets, and because different stakeholders will have different needs for the data products produced by the system, legal agreements will likely need to be different for individual-level vs. aggregated or de-identified data. Data requests for research purposes may require a different level of rigor and an ability to harmonize institutional review board requirements with data use agreements and frameworks. Originators of data used for public reporting may have still other requirements and restrictions.

Data Governance

Data governance encompasses the management and ownership of data within an organization. The processes associated with the ownership and management of data can be described as:

- The overall management of the availability, usability, integrity, and security of an organization's data;
- A system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who, what information, when, under what circumstances, and using what methods can action be taken;
- The people, processes, and information technology required to create a consistent and proper handling of data across an organization; and
- The activities that ensure data-related work is performed according to policies and practices as established through governance.[2]

Sustainable Financial Model

Financing models clarify funding sources, who is funding what, and how things will be paid for initially and ongoing. Health IT for Medicaid programs and for Medicaid participation in multi-payer programs and use cases can be funded by a combination of federal, state, and private sector funding sources through Medicaid financing programs. Some models include fees or subscriptions authorized by legislation or regulations. Decisions on funding often dictate the rules of engagement and may affect the scope of participation, and therefore should be developed in the context of other fundamental components of the eCQM solution.

Building shared health IT systems requires sustained, coordinated effort among stakeholders in a healthcare community because of the potential for volatility in state and federal health care policy, and due to the significant expense associated with building these systems. eCQM solutions require a similar level of effort to identify, plan for, and secure sustainable funding. Ensuring a long-term sustainable financial model is essential.

Until 2021, CMS may provide Medicaid match funds to support planning and implementation of approved projects at the Medicaid match rate of 90% with a 10% contribution from the State. Funding through the State Innovation Model programs can also be useful, but is time-limited through 2018.

---

[2] https://www.healthit.gov/sites/default/files/master_data_management_final.pdf

Over time, shared health IT services could be supported by a range of models with user fees, or state-sponsored fees, taxes, or assessments that are earmarked for health information exchange or interoperability activities.

Data Quality, Provenance, & Stewardship

Directories

Master Person Index

A Master Person (or Patient) Index facilitates the identification and linkage of patients' information across separate clinical, financial, and administrative systems, and is needed for information exchange to consolidate that information from various databases. This tool enables a holistic, often longitudinal, view of data that tells a story of how an individual passed through healthcare and service delivery systems.

It is critical for patient demographic data to be accurate and sufficiently populated in order to be effective elements for identification and linkage. Many demographic attributes can change over time, such as a last name (due to marriage) or a home address (after a move). In addition to these demographic changes, data-entry errors, such as misspellings or transformation of data, can inevitably cause variability in the records, described as data quality issues.

Master Provider Directory

A health provider directory describes the format and structure of information about individual and organizational health providers, and characteristics of those providers, including type, unique identifiers, practice specialty, and physical and electronic contact information. It supports management of healthcare provider information, authorizing and verifying providers, and linking providers across systems.

Examples: Information about the provider (demographics, physical addresses, credential and specialty information, as well as electronic endpoint to facilitate trusted communications with a provider); information about the provider's relationships (affiliation with other organizations and providers; Health Information Exchange (HIE) and members; Integrated Delivery Networks and care delivery members; hospitals and their practitioners; hospital sub-organizations including departments, physician Practice Groups and their practitioners, practitioners and the hospitals they are associated with).

Authorized User Management

Ensuring appropriate access to data should be controlled by both policies and technical tools that define and manage access to data based on individual and organizational roles of system users.

Attribution

Attribution is a process or function for matching patients to providers for purposes of care delivery and/or alternative payment models. Rules-based algorithms are employed to follow a general prospective or retrospective approach. Payers use this approach, but it requires the functionality of a Master Person Index and a Provider Directory.

Systems that allow for proper retrospective and prospective attribution of patients to providers aid in assigning cost and quality accountability under new payment models; they support providers in knowing to whom they are responsible for delivering care, and they aid in confirmation of notification or reporting of patients across health systems.

Secure Data Exchange Standards

Standards for health IT systems are developed through national and international organizations to support data exchange activities, including submitting data for quality measurement. Data will need to flow between a variety of clinical and non-clinical systems to measure quality and cost across the healthcare ecosystem in Connecticut (EHRs, lab systems, imaging systems, etc., as well as web-based systems. Some of the exchange modalities that could be used between contributing data systems and a statewide eCQM measurement system are:

Direct[3] is a specific assortment of technical standards that provide "push-based" messaging similar to secure email between EHRs and other systems, with clinical document attachments.

- Query/retrieve: Various technical standards that allow for identifying where clinical data for a specific person or people may be located within many different EHR systems, or within a central data repository, and also allow for pulling data from those systems into another system.
- HL7 v2: Collection of HIE-focused standards that provide a general framework that can support both *push* and *pull* technologies

HIPAA Requirements and Consent Framework

A system, process, or set of policies that enables patients to choose what health information they are willing to permit their healthcare providers to access and share. Consent management addresses participation in electronic health initiatives such as patient portals, personal health records (PHR), and health information exchanges (HIE). Risk-based planning and implementation of privacy and security practices will enable the program to identify the priority **safeguards** as early as possible, and build privacy and security into the design of the technology or business processes.

[3] https://www.healthit.gov/policy-researchers-implementers/direct-project

States face two key consent management issues: Basic Choice vs. Granular Choice (including opt-in vs. opt-out), and challenges related to federal regulations on the Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2).

The original HIPAA legislation has been modified and its regulation has been clarified, especially by the ONC Office for Civil Rights.[4] Guides[5] are available from authoritative sources, for example, to help individuals and institutions understand permitted uses and disclosures for clinical research[6] or keeping health information secure on mobile devices.[7]

In order to encourage eCQM stakeholders to engage with and agree to the obligations required by HIPAA and described in Data Use (or Sharing) Agreements, some governance frameworks generate a customizable privacy and security toolkit through a Technical Assistance Framework to help stakeholders refresh their existing privacy and security programs. This toolkit should include customizable sample policies and procedures, with placeholders for stakeholders to insert their organizational names, logos, and other specific information.

Privacy & Security Standards

In order to safely use and disclose health information for the purposes of health monitoring and improving health outcomes, as well as complying with the HIPAA privacy and security requirements that apply to entities involved in the eCQM solution, stakeholders need to, at a minimum:

- Establish a privacy and security governance model and supporting agreements among participants of the eCQM solution;
- Perform a Privacy Impact Assessment (PIA) on the conceptual, as well as the final, information inventory;
    - Including a third-party statistical analysis of potential for re-identification if de-identified data is used in the eCQM solution; and,
    - Including an analysis of what information and system documentation is potentially subject to or exempt from Freedom of Information Act (FOIA) requests;
- Identify all intended data flows and privacy or security safeguards required for those flows;
- Identify baseline privacy and security safeguards for the hosting of the data that is collected, used, and disclosed;
- Identify any privacy or security risks inherent in the hosting of the data that is collected, used, and disclosed;

[4] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
[5] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
[6] https://www.hhs.gov/sites/default/files/exchange_health_care_ops.pdf
[7] https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

- Identify any risks in the processes and mechanisms used to collect, use, and disclose the data; and
- Identify, implement, and deploy any additional administrative, technical and physical safeguards required to protect the data.

Risk-Based Privacy and Security

One of the most cost effective approaches to implementing privacy and security is the risk-based approach. Risk-based privacy and security refers to the process of targeting and prioritizing privacy and security processes and technologies to where they are most needed, in other words, the biggest risks with the highest probability of the most harm are the ones where the majority of time and resources are spent protecting against them.

A robust privacy and security assessment process enables a program to identify the priority safeguards as early as possible and build privacy and security into the design of the technology or business processes, rather than engaging in expensive and time-consuming reactive privacy and security measures. Risk-based privacy and security implementation also permits a program to tailor their spending on protecting priority assets using the most optimized protections, based on detailed analysis rather than high-level regulatory requirements.

Best practices for risk-based privacy and security implementation include:

- Systematic evaluation of information and technology assets;
- Application of privacy principles of transparency, limited collection and disclosure, safeguarding, and other privacy concepts to assets;
- Identification of potential risks to assets;
- Prioritization of risks using likelihood and impact assessment; and,
- Implementation of governance, technology and process safeguards to reduce risks.

The purpose of identifying risks is to plan how to mitigate, or reduce them. Once risks are prioritized, the high priority risks must be addressed using a combination of responses, referred to as safeguards or mitigations. Mitigations traditionally fall into these categories:[8]

- **Administrative safeguards**: Administrative safeguards include agreements, policies and procedures that can be used to reduce the likelihood of a risk occurring such as training staff in the proper handling of PHI. Administrative safeguards such as purchasing insurance can also be used to reduce the impact of a risk and cost.
- **Physical safeguards:** Physical safeguards include any modifications to the physical environment to protect the privacy or security of the assets, such as locked doors, privacy screens, private rooms for patient consultation, and fingerprint scanners. Even fire-suppression systems can be important components of reducing privacy or security risks.

[8] https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

- **Technology safeguards:** Technology safeguards include any technical means to protect and reduce the risk to assets, such as encryption, access control and audit technologies.

While encryption and access controls are critical components of secure IT implementations, mitigations such as privacy and security awareness and training are key to ensuring that technology is used properly, and that information is managed correctly outside of the technology. Additionally, governance procedures such as data use or sharing agreements, and reporting or enforcement procedures are necessary in order to scale privacy and security processes across broad networks of organizations that share information assets. In other words, a holistic, risk-based approach to selecting a combination of administrative, physical, and technology safeguards will be less costly and more effective at reducing privacy and security risk than procurement and installation of costly technologies alone.

Privacy Impact Assessment and Threat and Risk Assessment

A Privacy Impact Assessment (PIA) and a Threat and Risk Assessment (TRA) are the traditional means for assessing privacy and security risks to sensitive information and technology assets. Once risks are identified in PIAs and TRAs, those risks are prioritized, and appropriate mitigations are assigned based on priority. Privacy and security risks assessments should follow an approach such as that outlined in NIST 800-30 or equivalent standards,[9] or those recommended by the Health Information Management Systems Society (HIMSS).[10] PIAs and TRAs should plot risks along a heat map, or use a more quantitative method to prioritize privacy and security risks, and subsequent mitigation spending.

A "delta" (Δ) PIA and TRA is the term commonly used for an updated version of the PIA and TRA assessment conducted during the planning phase. The ΔPIA and TRA assesses the reductions or increases in previously identified risks caused by decisions and technology selections made during the design phase. The ΔPIA and TRA may also identify new risks introduced by any new technologies or design changes made during the design of the eCQM solution.

Quality Controls and Content Standards

Quality Controls and Content Standards are developed under business processes and/or technical solution documentation to ensure the integrity of an organization's data during collection, application (including aggregation), warehousing, and analysis. Processes to improve the quality of data may include on-site practice transformation technical assistance and use of data quality provider feedback and reporting tools.

[9] https://www.iso.org/isoiec-27001-information-security.html
[10] https://www.himss.org/files/HIMSSorg/content/files/D87_HIMSS_PIA_Guide_.pdf

Data Provenance

Data Provenance in the context of health IT refers to evidence and attributes describing the origin of and changes to health information as it is captured and transferred across different systems. Design of an eCQM solution may include describing information flows for many reasons but also to:

- trace and verify the creation of information,
- describe how data has been used by or moved among different databases, and
- describe how it is altered throughout its lifecycle.

Visibility into how data elements were captured and transformed is an important feature in IT systems that earns the trust of data users.

Data Dictionaries

Organizations that manage data must create and maintain a source of truth describing the contents, format, and structure of field names (their length, formats, encoding terminology, description and other information) used in different databases and the relationship between common data elements across systems. These dictionaries may also be used to control access to and manipulation of the database.

Data Extraction, Transformation, & Aggregation

Data Normalization, Integration, & Analysis

Data transformation converts a set of data values from the data format of a source data system into the data format of a destination data system. There can be multiple steps involved in this process, including data mapping, code generation, and data normalization to reduce data redundancy and improve data integrity.

Risk adjustment

Risk adjustment is a method used to calibrate health plan payments based on the relative health of the at-risk populations. Factors such as patient age, disability, existing health conditions are considered in determining payments and are used to stratify a population by health risk to target care.

Reporting services and tools

Analytical Tools

Analytical tools include services that take in data and use that data to support users in creating new knowledge or actionable insights based on analysis, usually using statistical methods.

Analytics services perform data analytics capabilities and can work in conjunction with reporting services by reporting out the analytical developed information in reporting formats. These software tools may be more sophisticated than typical reporting tools, and may require skilled users (statisticians, informaticists) to interpret the data and the results, and to generate reports.

Notification

A class of services that act on the status of messages, or on a status change flag, to either forward a message or create an appropriate message from the content received, with distribution based on a rule set to determine who gets what message.

Event notifications (e.g., Admission, Discharge and Transfer (ADT) "alerts") are one instance of notification services, ideally combined with analytics services and filtering capabilities to allow for customized alerts notifying targeted users of specific information related to an event.

Examples: ADT "alerts" notifying a care team of ER visit or hospital admission/discharge; event notifications of other services, including services that impact health as well as notification of use of need for a health care service. Potentially a notification could be linked to authorization.

Consumer tools

This is a category of services available to consumers to view and manage their health information or information about themselves. An example of the former is accessing lab results. An example of the latter is choosing preferences in a consent registry for sharing their health information.

Examples: Patient education, engagement and access tools, in addition to patient portals. Mobile health applications.

Provider tools

Like consumer tools, provider tools can provide information about or related to patients, such as longitudinal clinical results, but can also allow a provider to manage provider information, or other information of importance to the provider, in a provider registry or other application. Providers may be able to compare outcomes of their patient panels to similar organizations or communities in an anonymized fashion.

Examples: Dashboards, feedback reports, informed decision-making tools, provider education portals, Provider education, engagement and access tools. Mobile health applications. Quality Measure Feedback portals: feedback reports sent into EHRs to be used in cooperation with quality improvement technical assistance.