CareSpark Responses

While responding to the questions below, it is recommended that each response identify 1) the risks and benefits associated with a particular identity proofing and/or user authentication method; 2) the potential costs and/or barriers associated with the method's implementation; and 3) if feasible, quantify the risks, benefits, costs, or barriers discussed in parts 1 and 2, with respect to a health care consumer, provider, other entity, or all. *Reponses should be particularly focused on the Community's breakthrough regarding access to current and historical laboratory results and interpretations in an electronic health record (EHR).* Where possible, please provide references to any peer reviewed literature that has informed your response.

1. **Based on your experience (personal/organizational) with EHR technology, that can at a minimum provide access to current and historical laboratory results and interpretations, should identity proofing and user authentication methodologies (technical, policy, and implementation) differentiate based upon:**
    a. **The reception method of the data**
    b. **For example: accessing a laboratory's secure website for results and typing them into a patients EHR vs. automatic population from the lab to the EHR; and**
    c. **The interconnectivity of the EHR**
    d. **For example: a doctor in a large health care system may be able to query another provider's EHR for data as opposed to querying the lab directly.**

Providers in the CareSpark region (northeast Tennessee and southwest Virginia) have indicated a strong preference for single sign-on authentication to a portal / viewer that allows access to an integrated presentation of data from multiple sources, in contrast to switching between multiple portals and manual entry of data from one system to another. Identity proofing and user authentication should be consistently administered so as not to place undue burden on provider organizations; two-factor authentication has been recommended by those with technical and legal expertise in privacy and security compliance.

2. **If private industry EHR services were to import data from Federal agencies (who are required either by statute or policy to protect data in certain ways), would it be reasonable to expect that the EHR service provided would comply with Federal information security practices?**

While EHR vendors may be required to support federal information security practices through their products, it is unrealistic to expect that all provider organizations can or should be required to comply with these same practices. The cost for EHR vendors to adapt products to meet federal information security practices may result in increased prices for EHR systems, thereby inhibiting provider adoption and excluding small provider organizations from participating in health information exchange. Regulatory requirements should be appropriate to the size and resources of the organizations engaged in serving health care needs, so that there are not undue burdens--and thus unintended consequences--that reduce rather than increase the number of providers participating in health information exchange.

3. **For an EHR that will, at a minimum, provide access to current and historical laboratory results and interpretations, should there be different identity proofing and user authentication processes for:**
   a. **A patient versus a clinician. If yes, please explain and identify the scenario**

   Patient identity is affirmed by the clinician who has a direct relationship with the patient, either by reasons of personal acquaintance and / or valid documentation. Clinicians with indirect relationship (ie, labs or other clinicians who have received referrals) and the health information exchange organization must be able to assume that patient identity has been verified and affirmed by the referring clinician.

   Clinicians must be authenticated for appropriate levels of access, affirming their role and relationship with the patient whose information is being shared. In addition, clinicians should provide name, location / address of care delivery, and unique provider identifier, validated through a process using two-factor authentication (user name and password, token or PKI). Initial application for and approval of clinician authentication should include valid photo ID, which should be stored electronically (scanned) in a secure manner.

   Authentication should be re-validated periodically, as determined by the business practices of the provider organization and / or health information exchange infrastructure. To reduce administrative burden and cost, health information exchange organizations should allow and enable federated identity management, accepting validated users from "trusted entities" whose user authentication policies and practices meet required standards.

4. **For an EHR that will, at a minimum, provide access to current and historical laboratory results and interpretations, what/how do you see HHS' role, if any, in establishing guidelines for the health care industry with respect to identity proofing and user authentication? Or should the industry self-police in this area?**

   Existing products for federated identity management are available, and should be considered as viable options for use in the healthcare industry. EHR vendors and users should be encouraged to adapt products and practices to take advantage of these existing resources, rather than investing in development of products narrowly focused on the healthcare industry. Market forces will result in voluntary movement to interoperable products, but HHS could and should facilitate collaboration to this end, where and when feasible.

5. **For an EHR that will, at a minimum, provide access to current and historical laboratory results and interpretations, does an in-person identity proofing process provide greater benefit than automated, on-line processes, or vice-versa? Please explain.**

   In the CareSpark region, a survey of 169 members of the general public in March – May 2006 revealed a strong preference by patients to authorize sharing of their personal health information via written forms at the physician office, as follows:
   92% indicated they would be willing to sign a written form at the physician office
   19% indicated they would be willing to sign a written form at another location
   16% indicated they would be willing to sign up on-line
   While this survey was not conducted as a statistically validated tool, it does lead to further inference that in-person identity-proofing of patients would be preferred.

   For clinicians, initial identity-proofing should be done in person at the provider organization, which could then allow automated, on-line authentication for "trusted entities", ie provider organizations who comply with approved standards, established and monitored by the health information exchange organization and / or an independent third party (VeriSign, RSA or others).

6. **For an EHR that will, at a minimum, provide access to current and historical laboratory results and interpretations, are there other industry policies and practices related to identity proofing and user authentication that could be used successfully in any of the Community identified breakthroughs (see above)? If so, please describe these policies and specify how these could be implemented in a way that would minimize the risks and maximize the benefits as well as how they would compare to alternative methods in terms of risks, benefits and feasibility of implementation.**

Here is how CareSpark approaches the issues and solution:

The Standard

Security controls are the management, operational and technical safeguards and countermeasures needed to protect the confidentiality, integrity and availability of a computer system and its information. Management safeguards range from risk assessments to security planning. Operational safeguards include factors such as personnel security and basic hardware/software maintenance. Technical safeguards include items such as audit trails and communications protection.

COBIT is designed to be employed not only by users and auditors, but also, and more important, as comprehensive for management and business process owners.

ITIL service management is concerned with delivering and supporting services that are appropriate to the business requirements of the organization for quality approach.

ISO 177999 An excellent code of practice for Information Security Management.

The National Institute of Standards (NIST) and Technology has defined mandatory minimum requirements for protecting federal data and computer systems. NIST published the security requirements March 14 as Federal Information Processing Standard (FIPS) 200.. NIS is very strong in accountability. A companion document, NIST Special Publication 800-53, defines a set of risk-based procedures for selecting security controls that satisfy those minimum requirements.

The Challenge

Federal Standards on what they should implement and how their chief information officers should test those implementations will be very costly for some EMR vendors and HealthCare Providers.

IT Risks

- Project Failure
- Wasted Investments
- Security Breaches
- System Crashes
- Failure by ISP to understand and meet customers' requirement
-

Need for a Framework of Best Practices

- To avoid reinventing wheels
- Reduce dependency on technology experts
- Increasing the potential to utilize less expiries staff with proper training
- Making it easier to leverage external assistance
- Overcoming nonconforming behavior
- Reducing error and risks
- Improving quality
- Improving ability to manage and monitor
- Increasing standardization leading to cost reduction
- Improving trust and confidence from management and partners
- Creating respect from regulators
- Safeguarding and proving values

CareSpark Solution

At CareSpark we understand that threats to information security are relatively young and there isn't a cookbook we can look at for what to do, therefore to ensure a cost-effective, risk-based approach to achieving adequate security across the RHIO, we try to improve our day-to-day security practices.

Care Spark discovered that in order to use standards and get best of it to support:

- Providing a management policy and control framework
- Enable process ownership
- Clear responsibility and accountability for IT activities
- Ensure return on investment
- Making sure significant risks has been identified and transparent to management, and responsibility for risk management that effective controls are in place
- Ensure resource have been efficiently organized
- Making sure IT activities can be monitored

It needs to tailor and combine best of all these Standards to:

1- Define requirement in service and project definition

- Setting clear IT objectives and metrics
- Creating Service Level Agreement (SLA) with Vendors
- Considering services and project portfolios collectively so that relative priority

2- Verifying provider capability

- Independent third party assessment
- Contractual commitment
- Attestations and Certifications

3- Facilitate maturity assessments

- Gap analysis
- Benchmarks
- Improving planning
- Avoidance of reinventing already proven good approach

4- Create a frame work for audit

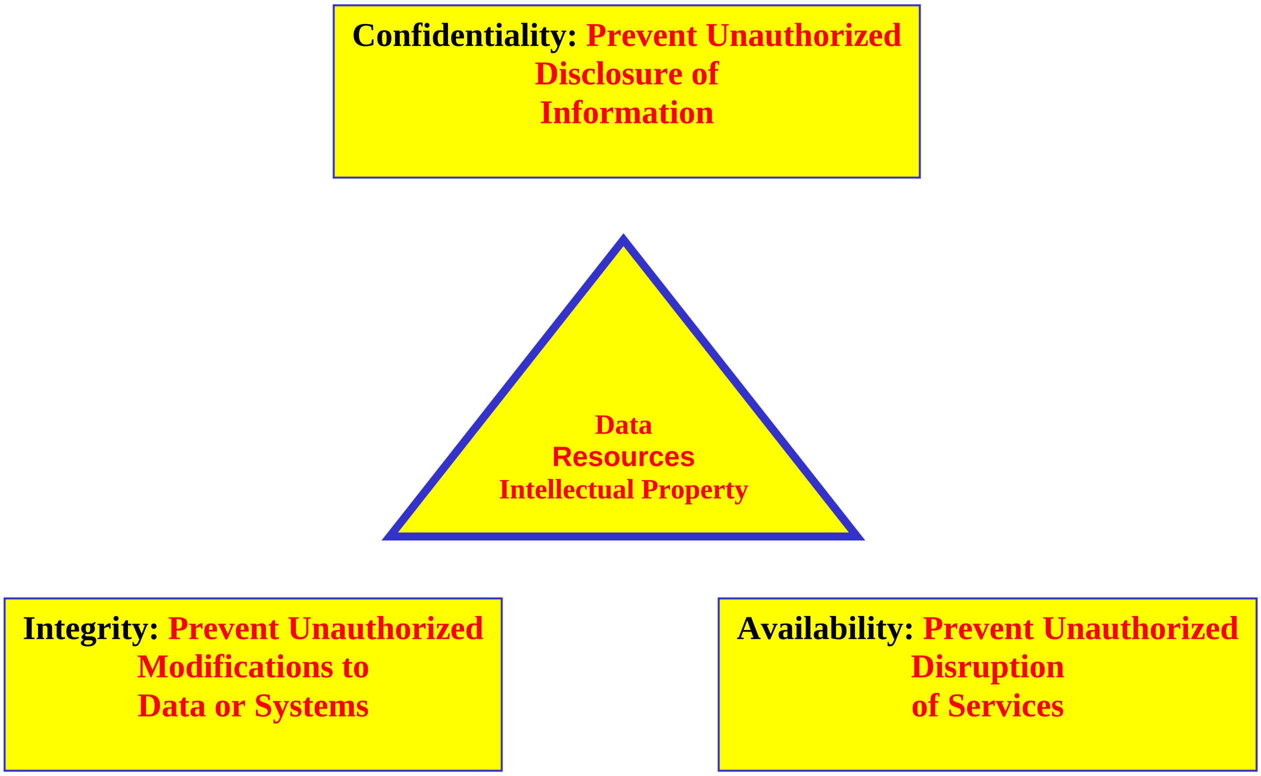
- Objectives and mutually understood criteria
- Benchmarking to justify and weakness and gaps in control
- Increasing depth and value of recommendations by following generally accepted preferred approaches

5- Implement minimal security

- Access control.
- Accountability and audit.

- Awareness and training.
- Certification, accreditation and security assessments.
- Configuration management.
- Contingency planning.
- Identification and authentication.
- Incident response.
- Maintenance.
- Media protection.
- Physical and environmental protection planning.
- Personnel security.
- Risk assessment.
- Security planning.
- System and services acquisition.
- System and communications protection.
- System and information integrity.

CareSpark Security Model


Confidentiality: Prevent Unauthorized Disclosure of Information
Data
Resources
Intellectual Property
Integrity: Prevent Unauthorized Modifications to Data or Systems
Availability: Prevent Unauthorized Disruption of Services

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept must be used to determine the overall impact level of the information system. Thus, a low-impact system is an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high. The determination of information system impact levels must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for those information systems.

CareSpark on HIPAA

CareSpark also understood that it needs to tailor and combine established security standards such as ISO17799, CBIT and ITIL, and NIST with the HIPAA regulation to provide a health-care focused profiling uniquely relevant to RHIO, and hire a third party to audit:

- **Risk Analysis**
  Review CareSpark's exposure to known threats.
- **GAP Analysis**
  Determine the existing state of CareSpark security challenges.
- **Policy and procedure review**
  Review of CareSpark security policies and procedures for compliance with HIPAA regulations.
- **Security assessment**
  Assess networks, systems and access for security weaknesses.
- **Standards Adherence**
  Analyze business against established standards using Industry Security Standards
- **Compliance Analysis**
  Review CareSpark compliance with relevant regulations.
- **Remediation Reporting**
  Report results of audit and develop remediation measures.
- **Implement Security Improvements**
  Architect and implement necessary security improvements.
- **Train & Educate Staff**
  Educate staff on proper security practices and procedures.
- **Certify compliance**
  Assess the effectiveness of security measures and certify their proper use.
- **Monitoring**
  On-going monitoring and validation to ensure compliance.

The result is a comprehensive process to increase the security and efficiency of CareSpark.

7. **For an EHR that will, at a minimum, provide access to current and historical laboratory results and interpretations, what is the appropriate balance of access to medical information in electronic form (through the use of stronger identity proofing and user authentication) against the privacy concerns of the consumer/patient? If possible, please discuss comparable programs/efforts in the past that have been successful in doing this?**

   In a general public survey conducted by CareSpark in March – May 2006, 169 respondents were asked to list the perceived benefits of electronic health information sharing. Benefits listed included the following:

   - Information when you need it
   - Communication with other doctors is an issue if doctor uses paper charts
   - Ease in changing primary care, advice of specialty
   - All have same information
   - Convenience
   - Technology error
   - Human error
   - Reduced duplication
   - Faster service for patient
   - Fewer mistakes
   - Helps make things better for all who work in the medical field, access to more patient info
   - Improved continuity of care, better coordination
   - Lessen multi-doctor, poly-pharmacy syndrome
   - A lot less paperwork, time spent finding charts
   - More accurate
   - Remote access for clinicians
   - Faster response time for lab, x-ray results

Respondents were also asked to list perceived risks, with the following responses noted:

a. Too many persons have access
b. Privacy and confidentiality is at risk
c. Pharmaceutical companies could use info
d. Inaccurate information available in situations where it is not needed (not life-threatening)
e. Technical error
f. Human error
g. Mistakes (such as when people have the same last name)
h. Misuse of information
i. Missing information
j. Something could be deleted with no way to recover records
k. Problems with “down time”

Of the 169 respondents, only 2 indicated that they would not give permission for their personal health information to be shared electronically, leading to the conclusion that the large majority (more than 98%) perceive the benefits to outweigh the risks.

8. **For an EHR that will, at a minimum, provide access to current and historical laboratory results and interpretations, should the health care industry adopt the concept of multiple assurance levels when performing identity proofing and user authentication functions, similar to what OMB has defined for the Federal Government in OMB Memorandum M-04-04? When responding to this question, please cite, if possible, other models that may exist specifically for health care?**

While increasing the security and protection of patient privacy, multiple levels of assurance could also pose significant barriers to provider adoption and use, severely impacting the functionality, cost and benefit of EHR's and thereby reducing the gains to be derived in health improvement and cost savings.

9. **For an EHR that will, at a minimum, provide access to current and historical laboratory results and interpretations, identify any particular concerns regarding the type of information collected for identity proofing or the storage of such information.**

Clinicians involved in CareSpark expressed strong concern and resistance to providing DEA numbers or other information that might allow misuse of their credentials, particularly for fraudulent prescriptions. They also expressed strong resistance to providing social security numbers or other information that could lead to theft of identity in financial transactions. Finally, their reluctance to provide home address, phone or email was attributed to concerns that they would be targeted by marketers of medical and consumer products, as well as patients who might infringe on their personal privacy.

People who responded to the general public survey conducted by CareSpark in March – May 2006 indicated a willingness to share information, as follows:
160 (94.6%) name, address, phone, date of birth
42 (24.8%) social security number
83 (49%) payment information (health plan, health savings account, credit card, or other)
103 (61%) employer
149 (88%) past history for health issues (childhood, previous illness or injury)
149 (88%) list of current medications, including vitamins, over the counter medications and
herbal supplements
141 (83.4%) allergies
141 (83.4%) names of physicians or other health professionals from whom you receive care

126 (74.5%) preferred choices for pharmacy, lab, diagnostic services, inpatient services
91 (53.8%) mental health diagnosis / treatment history
84 (49.7%) sexually-related diagnosis / treatment history
90 (53.2%) infectious disease history (HIV, tuberculosis, hepatitis)
112 (66.2%) chronic disease conditions (diabetes, lung disease, cancers)
130 (76.9%) family history of disease
2 (1.2%) none

Finally, members of the CareSpark Technology Team and Board of Directors have recognized the necessity of assuring that information from dis-enrolled patients not be released to or stored at the RHIO. A technical solution has been designed and is currently under development to manage Patient Option Preference at both the provider level (LPOP) and the RHIO levels (MPOP). (see attached design document)

Project: CareSpark MPOP/LPOP

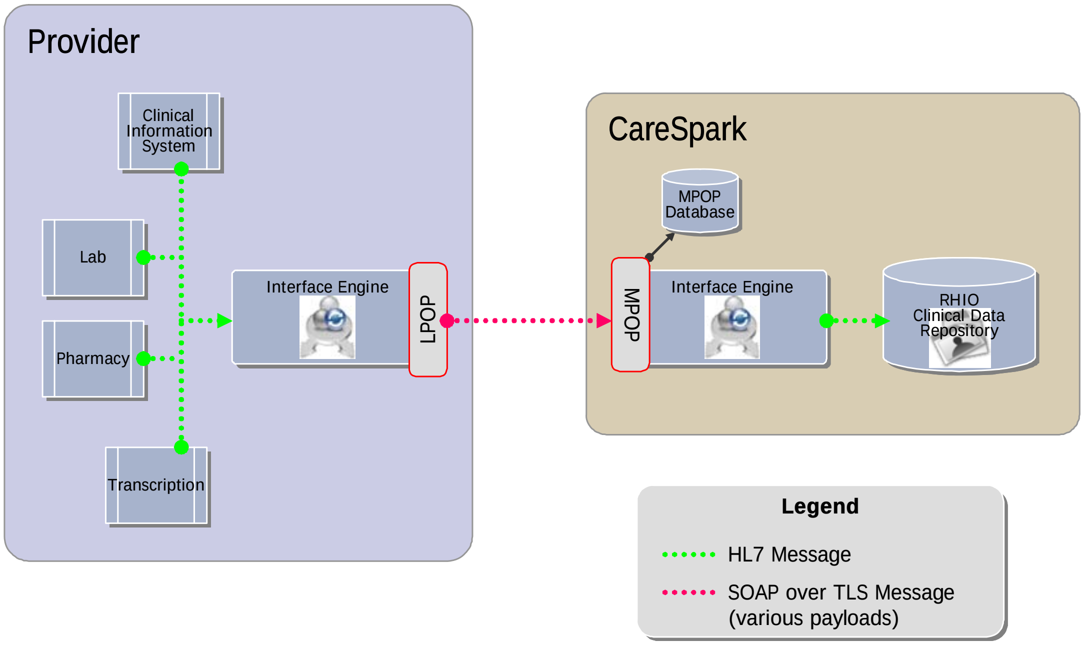
Objective
Provide patients control of record inclusion in CareSpark Clinical Data Repository. Ensure that when patients elect exclusion, no medical records from that provider are sent to CareSpark.

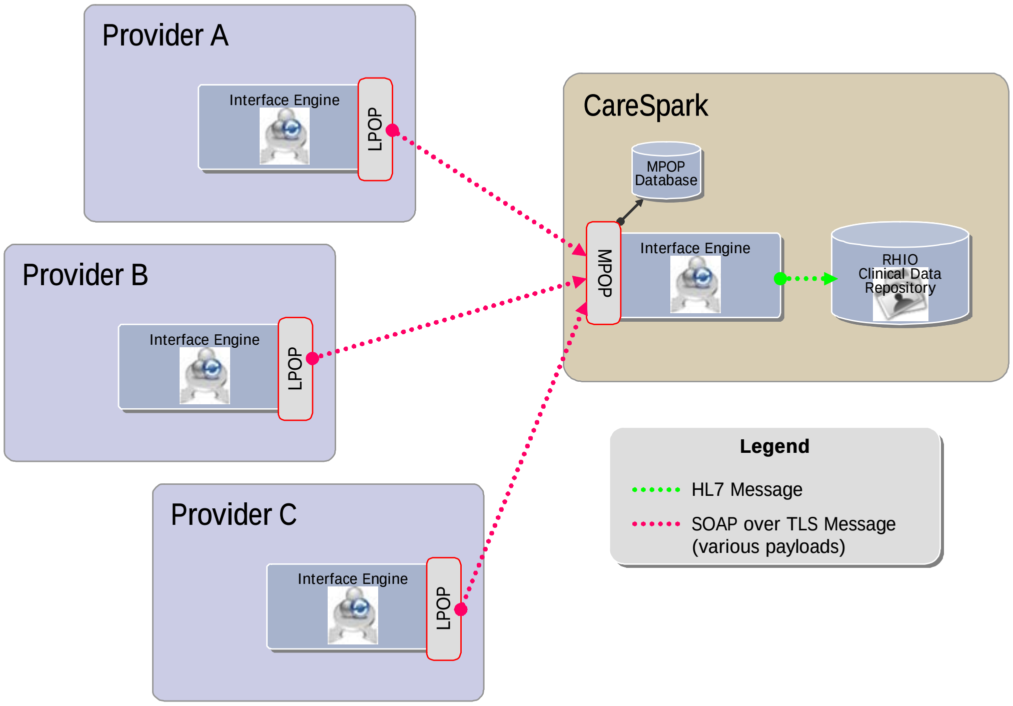
Factors
Each patient should control inclusion of their medical records. We are limited through both financial and practical factors to the existing relationship network. We do not foresee (at this time) a central organization that will authenticate and distribute PIN or other credentials to patients. Instead, we favor leverage of the existing infrastructure.

Patients are accustomed to signing information disclosure forms. We require a system that leverages this established practice and, equally importantly, the established contact point and confidence of this practice.

If the patient elects not to participate in CareSpark, we must ensure the patient's data is not transmitted.

The system should be low-profile, with minimal (or zero) maintenance required by the provider's network services post-deployment.


Provider
Clinical Information System
Lab
Pharmacy
Transcription
Interface Engine
LPOP
CareSpark
MPOP Database
MPOP
Interface Engine
RHIO Clinical Data Repository
Legend
HL7 Message
SOAP over TLS Message (various payloads)

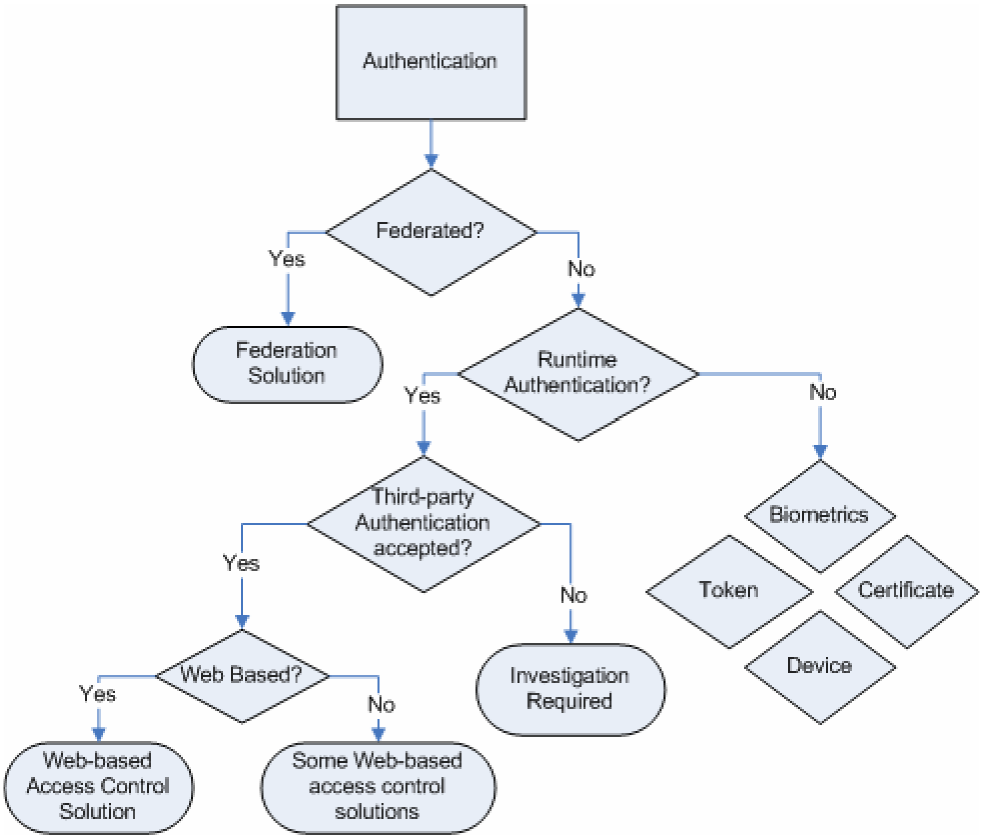

Provider A
Interface Engine
LPOP
Provider B
Interface Engine
LPOP
Provider C
Interface Engine
LPOP
CareSpark
MPOP Database
MPOP
Interface Engine
RHIO Clinical Data Repository
Legend
HL7 Message
SOAP over TLS Message (various payloads)

Authentication models

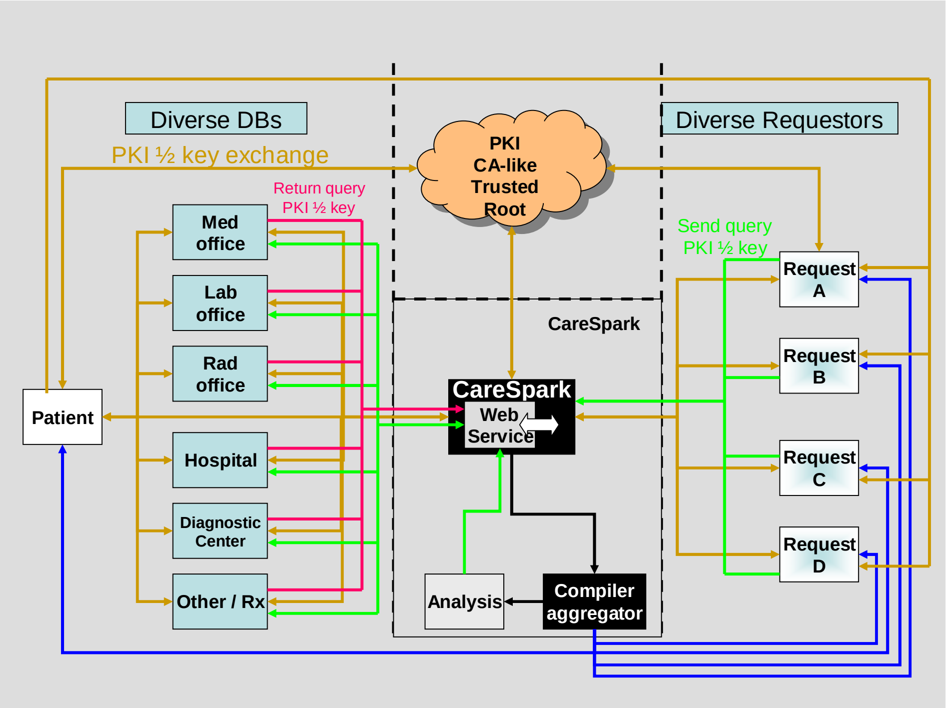
Caveat: While authentication is important, it is only one component of the MPOP.

There are at least 4 viable authentication models with potential applicability for CareSpark.
CareSpark will likely use a combination of Federated (Use of SAML) and Web Services (Use of PKI) in the near-long term.

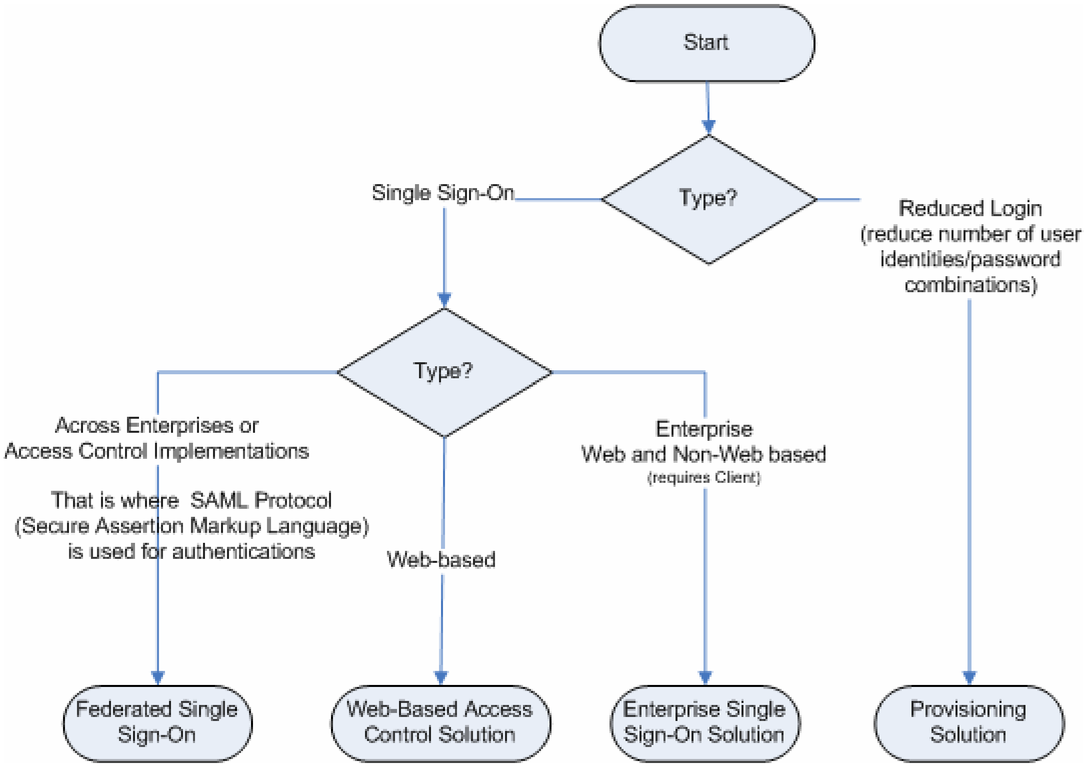
Authentication Methods



Unidentifiable Specific Data Aggregation –PKI based



Variables SSO



LPOP Design

The provider's interface engine requests transmission authorization from the LPOP. The LPOP in turn makes a secure outbound request for authorization from the MPOP, and authorizes or denies the interface engine's transmission.

CareSpark must deliver an LPOP component that works universally with any interface engine. Therefore, the key functionality of the LPOP must remain outside the interface engine. Interface engines must initiate calls to the LPOP for authorization prior to transmission of each record.

All participating organizations must have an interface engine of some type, although the engine may be custom-developed or vendor provided. The basic components recommended for participation include:

- Guaranteed messaging
- Message monitoring
- Interface connectivity monitoring/alerts
- Secure transmission of records
- Integration with LPOP for patient-level transmission authorization
- Transmission logging

Notes regarding record transmission:

We initially considered making the LPOP the transmission gateway between the interface engine and CareSpark. We determined this approach would not fully leverage significant capabilities of the interface engines. This would require development of guaranteed messaging, extensive logging, etc within the LPOP (as shown above), and further would not be as useful to organizations that already have significant expertise with managing the transmission of data through their own interfaces. Therefore, the LPOP focus transitioned from "gateway" to "gatekeeper". The LPOP does not transmit patient records; it simply authorizes the interface engine to transmit these records to CareSpark.

Notes regarding LPOP/MPOP division of services:

Early on, we determined that the LPOP should maintain a minimal footprint. A small footprint is beneficial in encouraging providers to add the application to their network, and in the event CareSpark elects to distribute a hardware agent (PC) to add to the provider's network, the smaller footprint reduces the requirements on this agent (and therefore cost).

Thus, the processing of authorization, with business logic, etc is primarily performed by the MPOP with the LPOP transmitting data to the MPOP and authorizing the interface to transmit based upon the MPOP response.

LPOP Configuration file

This simple xml file contains configuration settings for the LPOP to enable the deployment team to deploy the application without changing core functionality. As we learn more about the requirements for deployment and management we will use this configuration file to customize the installation.

Data elements

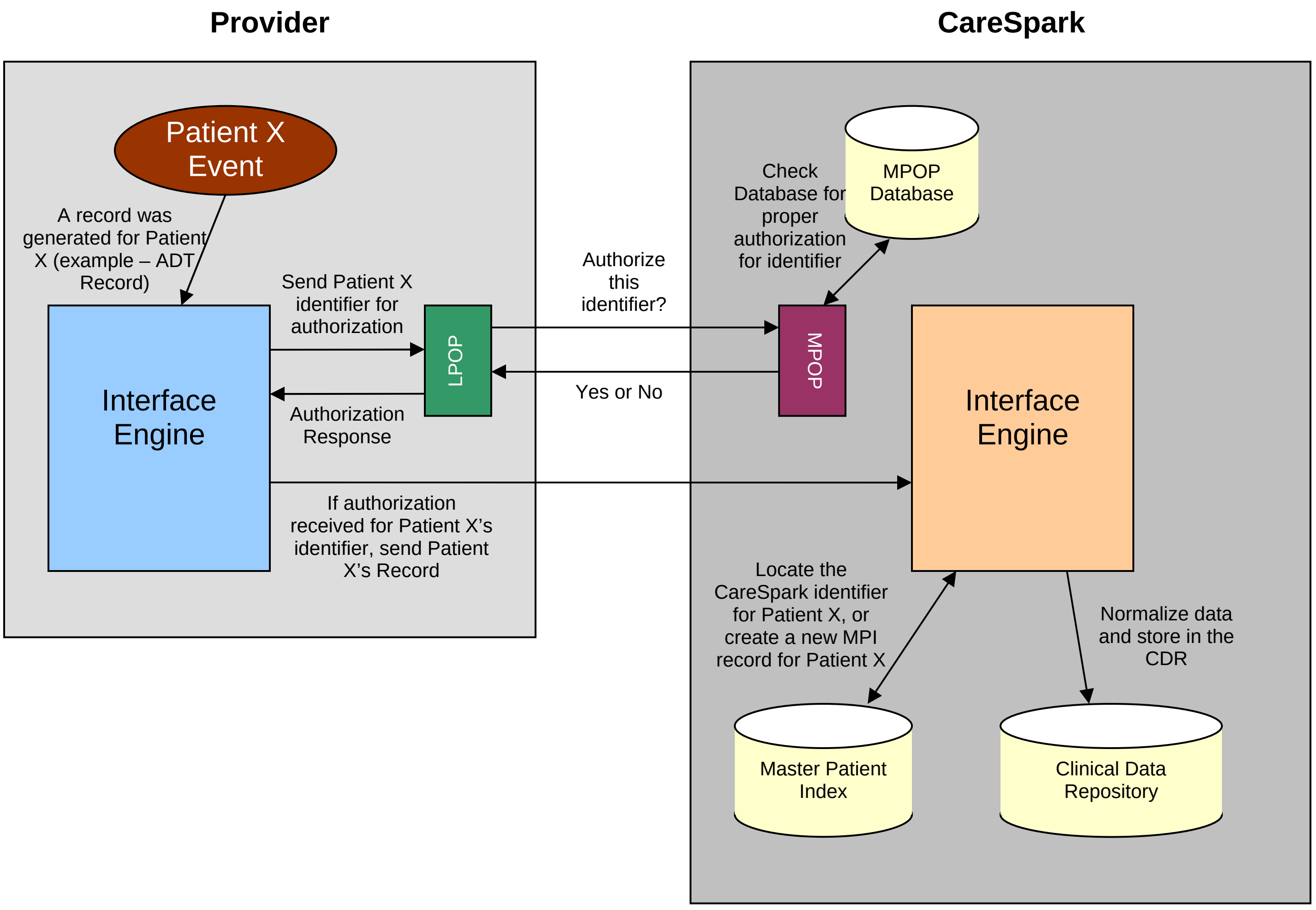
- MPOP Server address (IP Address)
- Local Administrator (eMail address)
- Provider identity (identifies the provider to MPOP)

LPOP Security (Formatting/cleanup remains)
All LPOP communications must be secured.

The web services transactions will all be encrypted and authenticated by mutual authentication TLS. An X.509 certificate issued by a CareSpark recognized certificate authority will need to be installed on any provider-side LPOP server that intends to communicate with the MPOP. The MPOP will as well have a certificate. Communications between these servers will be authenticated and encrypted.

Requests made to the MPOP without TLS, or with an invalid certificate must be rejected and not even acknowledged.

The LPOP will not accept inbound communication requests.


Provider
CareSpark
Patient X Event
A record was generated for Patient X (example – ADT Record)
Interface Engine
Send Patient X identifier for authorization
LPOP
Authorization Response
Authorize this identifier?
Yes or No
If authorization received for Patient X's identifier, send Patient X's Record
Check Database for proper authorization for identifier
MPOP Database
MPOP
Interface Engine
Locate the CareSpark identifier for Patient X, or create a new MPI record for Patient X
Normalize data and store in the CDR
Master Patient Index
Clinical Data Repository