# Introduction

Next generation Health Information Exchange (HIE) leveraging Standard Health Record. Initial versions have no PHI and instead will have synthetic patients within Massachusetts representative of the overall patient profile within the state.

Currently called SyntheticMass but need a new name as it grows into a full HIE. Possible names:

* SHR HIE
* Open Source HIE aka OSHIE
* NGHIE for Next Generation HIE
* HIR for Health Information Repository
* OpenHIE

# Sources

<https://www.paehealth.org/images/pdf/PA_eHealth_Appendix_M_-_Use_Cases.pdf>

<http://calhipso.org/documents/HIE_Toolkit_06.30.2013.pdf>

MassChallenge HIE Infrastructure Schulz edit 6-16-161.docx by Schulz, Kris

10x HIE 72416.pptx by Schulz, Kris

# Milestones

## WPI Digital Health and IoT Innovation Forum Demonstration (12 September 2016)

### Event Details

* Monday, September 12, 2016
* 8:15 am - 3:30 pm
* 100 Institute Road, WPI Rubin Campus Center
* Worcester, MA 01609

### Script

Same as Governor Baker Demonstration below?

## Governor Baker Demonstration (15 September 2016 or later)

Census and synthetic statistic visualization for the following statistics at the county and county subdivision levels on a map of Massachusetts:

* Population
* Population density
* % male population
* % female population
* % Diabetes prevalence

SyntheticMass should contain at least 100k synthetic patients.

Viewing the list of synthetic patients within a selected geographic area (county or county subdivision) including filtering based on data value chosen

Viewing of a synthetic patient from the above list

Downloading a synthetic patient record in C-CDA format.

No authentication/authorization/privacy/integrity.

### Script

* Demonstrating early version of an HIE
* **Goal 1: Mass Challenge**
  + Barrier to entry high – can’t access real data
  + Provide an HIE with 7 million synthetic (realistic but fake) patients
    - Mirror statistical population profile of MA based on census data
    - Allow startups to interoperate with realistic data from a realistic HIE including real security and PHI protections
  + MITRE Synthea tool simulates patients to generate synthetic patients
    - *Demo: Show example patient*
* **Goal 2: MA State-wide HIE?**
  + What if all EHR vendors in MA were required to submit to a state-wide HIE?
  + Population health queries to help make policy decisions against current data
    - *Demo: show current web app*
      * *1. Census data on map at county (population and % diabetes prevalence)*
      * *Sub-county level (population and % diabetes prevalence)*
      * *2. Synthetic data statistics on map (population and % diabetes prevalence) – county level*
      * *3. Sub-county level (population and % diabetes prevalence)*
      * *4. Click on Boston (% diabetes prevalence selected)*
      * *5. View patient list*
      * *6. View patient (same patient as seen initially)*
    - *Show mock-ups of more advanced capabilities but as a sequence:*
      * *1. Landing page*
      * *2. Mission Control*
      * *3. Build Visualization (Map)*
      * *4. See Visualization in action*
  + Disease surveillance capabilities
  + Patients can help improve accuracy with direct access
  + Healthcare providers gain access to entire health record of patient to improve care
* **Goal 3: Nationwide HIE**
  + MA leads the way to a national HIE based on a standard health record

## Start of Mass Challenge – SyntheticMass v1 (October 2016)

The Mass Challenge runs from October 2016 to March 2017. See <http://masschallenge.org/>. This milestone corresponds to the start of the Mass Challenge.

### Data

MITRE will provide 7 million synthetic patient records that represent a cohort of patients that align with the demographics and population health statistics for major diseases aligning with the population of the state of Massachusetts. These patients will have a longitudinal history of data for demographics, vitals, encounters, conditions, allergies, and medications.

The diseases targeted for support in synthetic patients are from the 2013 Global Burden of Disease (GBD) United States profile, the Top 10 causes of YLL (Years of Life Lost)

1. Ischemic Heart Disease (done)
2. Lung Cancer (in progress)
3. Alzheimer Disease
4. COPD
5. Cerebrovascular Disease
6. Road Injuries
7. Self-Harm
8. Diabetes (done)
9. Colorectal Cancer
10. Drug Use Disorders (We’ll focus on Opioids)

Source: <http://www.healthdata.org/united-states>

***No PII or PHI will be supported within SyntheticMass.***

### Infrastructure

* Host syntheticmass.mitre.org in the DMZ for access from outside MITRE network
* Support OAuth2/OpenID
* Encrypted transport
* Encrypted PHI/PII data storage

### Functionality

Innovator Use Cases Available:

* 5.5.1 Visualize Census Data and Synthetic Population [Population Health, v1]

Support population, % male, % female, diabetes prevalence, plus 2 other conditions

* 5.5.2 Download Synthetic Patients [Patient Record, v1]

Only FHIR JSON and C-CDA formats will be supported initially

* 5.5.3 View Synthetic Patient [Patient Record, v1]
* 5.5.4 Integration Test My FHIR client [Patient Record, v1]

JSON format only

* 5.5.5 Integration Test My Direct Sending [Direct Messaging, v1]

Data will be in C-CDA format

* 5.5.6 Integration Test My Direct Receiving [Direct Messaging, v1]

Data will be in C-CDA format

* 5.5.7 Secure File Transfer (SFTP) C-CDA Synthetic Patient Records [Patient Record, v1]

## HIMSS17 Conference (February 2017)

The HIMSS Symposium is from February 19-23, 2017 at the Orange County Convention Center in Orlando, FL. A demonstration is planned for this event.

### Functionality

Use cases needed to demonstrate this complete patient story:

“Chronic condition, new (John Proctor Example)

A middle-aged man experiences a heart attack at home. He is transported to the nearest cardiac specialty facility where he undergoes cardiac stenting. While recovering in the ICU, he develops congestive heart failure as a complication of his heart attack. His condition is stabilized. He is discharged to a sub-acute rehabilitation facility, where he recovers for 1 week before discharge home. Home monitoring devices capture data on his body weight, medication adherence and blood pressure and transmit this to his Care Manager, Home Health Nurse and Primary Care Physician. He opts to receive his follow up care in the home, through teleconference involving the Home Health Nurse (in person), and the Primary Care Physician and Cardiologist (both present remotely).”

Source: <https://github.com/standardhealth/shr_spec/blob/master/PatientStories>

#### Health Professional

* 5.4.1 View Patient Record
* 5.4.3 Update Patient Record

## End of Mass Challenge – SyntheticMass v2 (March 2017)

By the end of Mass Challenge. Functionality based on feedback during Mass Challenge should take priority. Otherwise, functionality listed below will be implemented.

### Functionality

No new functionality unless high priority for Mass Challenge participants

## PHI Readiness Review (March 2017)

## HIE v1 Pilot(s) (October 2017?)

The HIE will need to be piloted within a small area. This pilot would be the first use of the HIE with PHI. Multiple pilots with increasing patient populations may be executed as well.

## HIE v1

Incorporate early version of SHR.

Initial cut of use cases for patient, health professional, researcher, and administrator.

Support for real data and synthetic data.

## HIE v2

Complete use cases for patient, health professional, researcher, innovator, and administrator. Initial cut of public health official, guardian, guest, and payer use cases.

## HIE v3

## National HIE Test Bed (?)

TBD

# Actors

## Administrator

Users who administer the SyntheticMass/HIE site will require access to administrative functions on the site

## Innovator

Vendors implementing new systems and technologies must interoperate with other vendors and require data for testing their systems. These users are referred to as innovators.

## Guardian

A patient will often have assigned guardians who are responsible for their medical care and therefore should have access to the patient’s health record.

## Guest

A user wanting to learn more about SyntheticMass/MA HIE should be able to access the site and learn about it without establishing an account.

## Health Professional

A health professional provides care to patients and gets paid for those services by payers. Health Professionals also purchase and use systems and software from innovators.

## Patient

A patient receives health care from health professionals.

## Payer

Payers are insurance providers. Payers sell insurance to patients and pay for patient care to health professionals.

## Policy Maker

A policy maker is someone in the government who influences health policies.

## Public Health Official

A public health official is someone representing a government health agency.

## Researcher

Researchers are professionals who use medical data to expand medical knowledge and hopefully improve care for patients in the future.

## Trial User

A trial user is someone showing the system to other people or a person directly trying out the system. A trial user is able to see the site as they would if they were a real user of a selected role. In other words, if I choose to be a trial patient user, I’d see the system as a patient would.

# Use Cases

## Administrator (secure web access)

### Manage Users [User Management, v1]

An administrator can add, view, update, and delete users from SyntheticMass.

### Lock/Unlock User Accounts [User Management, v2]

An administrator can lock or unlock user accounts.

### Archive Patient Data [Patient Archival, v2]

An administrator can choose to archive some patient-related data based on criteria. Archived data is removed from the primary tables and must be de-archived before it can be accessed again.

### De-archive Patient Data [Patient Archival, v2]

An administrator can put archived data back into the primary data store such that it is accessible again.

### Backup Data [Patient Backup, v2]

An administrator can initiate a backup or schedule periodic backups of data owned by the system. Any backed up data must be protected to ensure its privacy, integrity, and that only authorized users can access it.

### Restore Data from Backup [Patient Backup, v2]

An administrator can choose to restore data from backup into the active system.

### Log an Active User Out [User Management, v2]

An administrator can choose a currently logged in user and kick them out of the system.

### See Login Attempts [User Management, v3]

An administrator can view a log of login attempts (successful and unsuccessful).

### Notify if Failed Login Attempts Exceeds a Threshold [User Management, v3]

An administrator can receive a notification if failed login attempts from a single IP address exceed a certain number in a certain timeframe.

### Resolve Potential Duplicative Patient Records [Patient Matching, v2]

The administrator can go through a list of identified potential duplicative health records (see 5.12.8 Find Potential Duplicative Patients) and determine whether to merge them or mark them as not duplicates.

## Guardian (secure web and mobile access)

### View a Ward’s Patient Record [Patient Record, v3]

A guardian can view any of their wards’ patient records.

### Update a Ward’s Patient Record [Patient Record, v3]

A guardian can update some data in a ward’s patient record, and can request that other parts of it be updated as well.

### Identify Issue in a Ward’s Health Record [Issue Management, v3]

A guardian can identify a particular piece of data within a ward’s patient record that they think is incorrect and should be fixed.

### Handle an Informed Consent Request for a Ward’s Data [Informed Consent, v2]

A guardian is presented with a health professional’s request for access to one of their ward’s data. The guardian can consent or not.

## Guest (web and mobile access)

### Learn about HIE [About, v1]

A guest should be able to read about the HIE to learn about it and the SHR.

### Register with Site [About, v2]

A guest can request a login on SyntheticMass for a particular role (e.g., patient or innovator).

### View Public Health Data [Population Health, v1]

A guest can view public health data which consists of some aggregated statistics about all residents.

### View Standard Health Record Specification [About, v1]

A guest can get more information about the SHR including specifications.

## Health Professional (secure web and mobile access)

### View Patient Record [Patient Record, v1]

Health Professional must search for desired patient using patient identifiers. Health Professional may not have access to requested patient. View it on the site or have it send to their DIRECT e-mail address or download it in a specific format. Portions of record may not be visible to a health professional. Alternate course is when they don’t have access to the record or to a portion of it and they can request it.

Views of patient information should include a longitudinal view of the patient’s medical record over time.

### View Summary of Patient Record [Patient Record, v3]

A health professional can just see key data within an SHR to summarize a patient quickly.

### Update Patient Record [Patient Record, v1]

A health professional can update a patient’s record including adding new encounters, lab results, conditions, etc.

### Create Action for Patient [Patient Actions, v3]

A health professional can create an action for a patient which may be to make an appointment, weigh themselves once a week and record it in their SHR, log what they eat for a period of time, go get blood taken at a local lab, etc.

### Update myself in Health Professional Directory [Provider Directory, v2]

A health professional can update their direct e-mail address, regular e-mail address, phone numbers, street address(es), and other contact information in the health professional directory. They can also upload their certificates.

### Send Direct Message [Direct Messaging, v2]

A health professional can send a Direct message containing patient data.

Question: Does access to specific patient data always give a health professional permission to send it to someone via Direct?

### Look up a Health Professional in Directory [Provider Directory, v3]

A health professional can look up another health professional in the health professional directory in order to contact them (e.g., send a referral or lab results via Direct).

### Manage My Notifications [Notifications, v4]

Control what types of updates cause notifications (e.g., emergency room encounter) and the priority associated with the notification. Priority may also dictate notification mechanism (message on site at next login, e-mail, text message?)

### Receive Notification [Notifications, v4]

A health professional can define criteria under which data changes within the system will notify them and how they will be notified. For example, updates to any patient that they are defined as the primary care physician may result in an e-mail being sent to them. For another example, if any of their patients with a certain condition have an admit event, then the health professional is notified via text message.

### Address Potential Issues [Issue Management, v3]

The health professional views potential issues identified by a patient, guardian, or another health professional and disposes of them. Only health professionals with the ability to update the part of the patient record that the issue is associated with can address the issue. All health professionals with the ability to update the data that an issue is associated with will see the issue.

### View PDMP Prescription Drug History for Patient [Prescriptions, v4]

The health professional views the prescription drug history for a patient via the state’s PDMP.

### Prescribe a Drug for a Patient [Prescriptions, v4]

The health professional can prescribe a drug to a patient via an e-prescribing service.

### Request Access to Patient Data [Informed Consent, v2]

The health professional needs to access a patient’s health record in general or a specific subset of data within it and requests that access. This action could trigger informed consent process.

## Innovator (secure web access)

All Innovator use cases rely on synthetic data and never access PII or PHI.

### Visualize Census Data and Synthetic Population [Population Health, v0]

An innovator can view public maps displaying a statistic (e.g., population, population density, high school educated, living patients with diabetes, etc.) based on census data (where statistic is available) or synthetic data (where statistic is available). When viewing synthetic population statistics, a list of patients in a county or county subdivision that make up the selected statistic can be viewed and used to initiate a download (See 5.5.2 Download Synthetic Patients [Patient Record, v1]). In addition, from the list of patients, an individual synthetic patient can be viewed (see 5.5.3 View Synthetic Patient [Patient Record, v1]).

### Download Synthetic Patients [Patient Record, v0]

An innovator can download a list of patients using a selected format (CCDA, FHIR, or SHR implementation format). The downloaded patient record should be as complete as possible given the chosen format.

#### Basic Course

1. System displays list of patients (see use case 5.5.1 Visualize Census Data and Synthetic Population [Population Health, v1])
   1. User chooses to view list of synthetic patients
   2. System displays list of synthetic patients matching criteria
2. User requests to download the listed patients.
3. System offers user a choice of format.
4. User chooses an export format (CCDA, FHIR, SHR implementation format(s))
5. System creates export file in requested format containing matching patients and allows user to save it to their local machine

### View Synthetic Patient [Patient Record, v0]

An innovator can view the health record of a synthetic patient based on a list of patients generated from another use case (See 5.5.1 Visualize Census Data and Synthetic Population [Population Health, v1]).

### Integration Test My FHIR client [Patient Record, v0]

An innovator can test a FHIR client they are building against the SyntheticMass FHIR server with synthetic data.

1. FHIR client makes FHIR calls to system including authentication and authorization (SMART on FHIR)
2. System handles requests and responds per FHIR specification

### Integration Test My Direct Sending [Direct Messaging, v0]

An innovator can test their Direct implementation by sending a Direct message to SyntheticMass. Any data sent must be synthetic.

1. User sends a DIRECT e-mail to SyntheticMass
2. System reads and accepts the e-mail and its content (CCDA format).
3. System inserts the provided patient data

NOTE: early versions may not merge Direct data with FHIR or CCDA synthetic data

### Integration Test My Direct Receiving [Direct Messaging, v0]

An innovator can test their Direct implementation by telling SyntheticMass to send it some synthetic data.

### Secure File Transfer (SFTP) C-CDA Synthetic Patient Records [Patient Record, v0]

An innovator can use SFTP to browse and download synthetic patient records in C-CDA format. How will security work for this? Can Ubuntu use OAuth2 and OpenID Connect? Also, we can’t have 1 flat directory with 7 million XML files in it. How will be organize them? Are all 7 million available via SFTP?

### Test Interoperability of FHIR Client [Patient Record, v4]

An innovator can test their FHIR client by executing a defined compliance test suite using SyntheticMass as the server-side that will validate the client requests are correct and then return expected results as defined in the test suite.

1. FHIR client makes each predefined call from test suite
2. System responds with response
3. FHIR client validates that response is correct per test suite

### Test Interoperability of FHIR Server [Patient Record, v4]

An innovator can test their FHIR server by initiating the client compliance test suite via SyntheticMass. SyntheticMass will then proceed to invoke each test case in the suite and validate the responses.

1. User initiates test suite for a provided FHIR service endpoint
2. System executes test suite and verifies each response and presents user with results

### Test Compliance of a Standard Health Record Instance [Patient Record, v3]

An innovator can provide an instance of a Standard Health Record and SyntheticMass will assess its compliance and provide a report.

1. User provides an instance of a Standard Health Record
2. System identifies the format and version of the Standard Health Record provided and validates that the instance complies with the standard
3. User acknowledges that the instance was in compliance

## Patient (secure web and mobile access)

### View My Health Record [Patient Record, v1]

Patient can view their own Health Record on the site or can download it in an encrypted, password protected format allowing them to provide their current Health Record to a health professional without access.

### View Audit Log of Accesses of My Health Record [Patient Record, v2]

A patient can view all accesses of their health record. Should they have a way to question an access?

### View Provenance for any Data in My Health Record [Patient Record, v2]

A patient can view provenance (who and when the data was entered into the system) for any data within their health record.

### Update My Health Record [Patient Record, v3]

Depending on data being updated, an update may occur directly (e.g., patient address), require approval from health professional (e.g., adding an encounter that occurred while in a different country), or not be allowed (update an existing encounter).

### Manage Health Professional-Assigned Actions [Patient Actions, v3]

Add comments, status updates, and results to health professional-assigned actions.

### Identify Issues in My Health Record [Issue Management, v3]

Patient can add comments/questions to their health record including targeted questions to specific health professionals.

### Control Access to My Health Record [Patient Record, v3]

Health Professionals/Payers can request access and patients can change rules for who has access and to what parts of their record.

Issue: How long does consent last?

### Handle an Informed Consent Request [Informed Consent, v2]

A patient is presented with a health professional’s request for access to their health record or to a specific subset of it. The patient can consent or not.

### Opt-in to Clinical Trials I’m Eligible for [Clinical Trials, v4]

A patient can browse a list of clinical trials that they are eligible for (as defined by a researcher) and request to opt-in. Any data requirements defined for the clinical trial (by the researcher) will be placed on their health record. As part of opting in, the patient will also be consenting to access to specific portions of their patient record by the researcher.

## Payer (secure web access)

### View Subscriber’s Health Record [Patient Record, v4]

Payer must search for desired patient using patient identifiers. Payer may not have access to requested patient. View patient on site or have it sent to a DIRECT e-mail address or download it in a specific format. Part of the record may not be visible to payer.

### View Statistics Across Subscribers [Population Health, v4]

Payer can visualize statistics across their subscribers.

Question: Do we need the ability to save visualizations much like public health official but data would be scoped to subscribers for payer only? Or support comparison of statistics across subscribers to state-wide?

### Download Subscriber Data [Patient Record, v4]

Payer can download data (selected items from health record) for each matching subscriber (based on defined criteria) in CSV format.

### Upload Subscriber Data [Patient Record, v4]

Payer can upload updates to subscriber data in CSV format. Need to defined what parts of health record can be updated. Also, can subscribers only be updated? Does it make sense to create new subscribers (i.e. patients) this way? No delete support.

## Policy Maker (secure web access)

### Visualize Public Health Data [Population Health, v3]

A policy maker can visualize public health data in a graph or on a map. The policy maker can select statistics and overlay them on the same map or graph. Statistics can be demographic-based, social determinants of health, prevalence rates for conditions, incidence rates for conditions, and cost-based. Some statistics will be based on aggregating patient health records and others will be pulled from external sources. Policy makers can save visualizations they create.

### View My Dashboard [Population Health, v3]

A policy maker can see a dashboard summarizing the health of MA residents in ways of interest to them. Trending conditions, high volume locations, and other metrics will be shown.

### Manage Data Visualizations [Population Health, v3]

A policy maker can view, update, or delete their data visualizations. A policy maker can choose to promote a saved visualization to their dashboard.

### Manage My Notifications [Notifications, v4]

Set up standing queries that define conditions under which policy maker should be notified; e.g., a certain statistic passes a threshold value.

### Receive Notification [Notifications, v4]

The policy maker receives notifications when conditions that they define occur. See Manage Notifications. Notifications should exist on the site but ideally can be sent as an e-mail or a text message as well (with no PHI).

## Public Health Official (secure web access)

### Visualize Public Health Data [Population Health, v3]

A public health official can visualize public health data in a graph or on a map. The public health official can select statistics and overlay them on the same map or graph. Statistics can be demographic-based, social determinants of health, prevalence rates for conditions, incidence rates for conditions, and cost-based. Some statistics will be based on aggregating patient health records and others will be pulled from external sources. Public health officials can save visualizations they create.

### View My Dashboard [Population Health, v3]

A public health official can see a dashboard summarizing the health of MA residents in ways of interest to them. Trending conditions, high volume locations, and other metrics will be shown.

### Highlight Changes in Citizen Health Status [Population Health, v4]

A public health official can highlight significant changes in the health status of patients in the HIE.

### View Dashboard of Interoperability and Adoption Status [Adoption Metrics, v4]

A public health official can view a dashboard listing HIEs in a geographic area and their interoperability and adoption status. Each HIE must support a query which can provide back version information for a registered HIE.

### View Activity Metrics [Adoption Metrics, v4]

A public health official can view metrics related to traffic to one or more registered HIEs including logins per role type and health data in and out rates for examples.

### Manage Visualizations [Population Health, v3]

Visualizations created and saved in 5.9.1 Visualize Public Health Data can be viewed, edited, or deleted. Visualizations can also be put on the dashboard (see 5.9.2 View My Dashboard) or removed from it.

### Manage My Notifications [Notifications, v4]

Set up standing queries that define conditions under which public health official should be notified; e.g., a certain statistic passes a threshold value. Capability represents basic disease surveillance functionality

### Receive Notification [Notifications, v4]

The public health official receives notifications when conditions that they define occur. See Manage Notifications. Notifications should exist on the site but ideally can be sent as an e-mail or a text message as well (with no PHI).

## Researcher (secure web access)

### Analyze Health Data [Population Health, v3]

A researcher can analyze the aggregated health records by defining queries against the data. Specific patient identifying information will never be returned.

### Download Raw Data in CSV format [Patient Record, v3]

A researcher can query the patient data and download the results in CSV format. Specific patient identifying information will never be returned.

### Manage Visualizations [Population Health, v3]

A researcher can create, update, and delete visualizations that they own. Visualizations created by a researcher are private unless explicitly marked as public. Visualizations can present on a map, in a graph form (e.g., bar, scatter, pie, …), or on a timeline (?).

### View Visualizations [Population Health, v3]

A researcher can view their visualizations or any other public visualizations.

### Manage My Notifications [Notifications, v4]

Set up standing queries that define conditions under which researcher should be notified; e.g., a certain statistic passes a threshold value.

### Receive Notification [Notifications, v4]

The researcher receives notifications when conditions that they define occur. See Manage Notifications. Notifications should exist on the site but ideally can be sent as an e-mail or a text message as well (with no PHI).

### Add Clinical Trial to Marketplace [Clinical Trials, v4]

A researcher can add a planned clinical trial to the marketplace to allow patients to opt-in. As part of defining the new clinical trial, the researcher identifies eligibility requirements that define what patients can participate. In addition, the researcher defines data collection requirements for participating patients. The researcher also specifies what portions of the patient’s health record they need access to for the clinical trial. The patient must consent to access in order to opt in.

### Approve Patient Participation in a Clinical Trial [Clinical Trials, v4]

A researcher can approve patients who have requested participation in a clinical trial. Opting in should include consent to view relevant portions of the patient’s health record.

## Trial User

### Use the System as if Logged in as a Selected Role [Trial, v3]

A trial user can choose a role (e.g., patient, health professional, researcher, etc.) and use the system as if they were logged in as a user of that type. All data access will use the synthetic data.

## Shared

These use cases are common across all roles (e.g., Provide Feedback) or are included by other use cases to satisfy non-functional requirements (e.g., Login).

### Login [User Management, v1]

Any user (except guest) should be able to login to their account by authenticating with SyntheticMass. Note that different levels of authentication may be required for different user types. If a user can play multiple roles, they should be able to select a default role or choose to pick each time they login through their user preferences.

### Provide Feedback [Feedback, v2]

Any user can provide feedback on SyntheticMass including potential enhancements.

### Request Support [Support, v3]

Any user should be able to request support with SyntheticMass if they are having trouble.

### Forgot Username and/or Password [User Management, v2]

Any user can indicate that they forgot their username and/or password.

### Change Password [User Management, v2]

Any user can change their password.

### Manage My Preferences [User Preferences, v3]

Any user can setup certain preferences only affecting their use of SyntheticMass. Current list of preferences:

* Default login role or if the system should ask for a user’s desired role for this session when they login.
* Inactivity Time Before Automatic Logoff
* User Interface customizations

### Switch Roles [User Management, v3]

A user that has multiple roles assigned can switch to a different role on the site. Only functionality appropriate to their current role should be available. Note that switching roles may require additional authentication.

### Find Potential Duplicative Patients [Patient Matching, v2]

The system should analyze health records and identify potentially duplicative records on a periodic basis. See 5.1.10 Resolve Potential Duplicative Patient Records for how an Administrator handles the potential duplicates discovered). Note that if two records were identified as potential duplicates and then an administrator subsequently indicated they were not duplicates, those records should not appear in future lists of potential duplicates unless changes have occurred?

## Missing Functionality?

1. Blue Button
2. ADT Tracking
3. ADT Alerts
4. Query-based Exchange
5. eHealth Exchange
6. EMS Care Coordination
7. Data Analytics
8. Patient de-duplication
9. May need additional actors for prospective health professionals/innovators/payers/researchers to try the HIE out?
10. Move Manage My Notifications and Receive Notification use cases to Shared and just give every role the ability to setup notifications for data they can access?

# Non-Functional Requirements

## Authentication/Authorization [Security, v1]

All roles but guest will require user authentication (2 factor for some roles and/or functions?) and authorization checks for functions being performed as well as for the data being accessed. Authentication and authorization will likely be at least partially accomplished using OAuth2 / OpenID Connect. See use case 5.12.1 Login [User Management, v1].

## Automatic Logoff After Preferred Time Period [Security, v2]

The system will automatically log a user off after a configurable period of time with no activity. The value is configured as part of the user preferences (Inactivity Time Before Automatic Logoff) with no ability to disable it. This use case helps with HIPAA compliance.

## Availability [Availability, v4]

The HIE must guarantee certain availability levels in a service level agreement with its users. TBD

## Completeness Scoring of Patient Health Records [Patient Record, v3]

Whenever a patient’s health record is viewed, a completeness score should be available. Providing the best patient data possible depends on the accuracy of the data. A “completeness” score is required to indicate to the patient and provider how complete, accurate and up-to date a patient’s health record is. This metric should exist in their SHR in an obvious place where it can be taken notice of by the provider and patient.

* <https://github.com/standardhealth/shr_spec/blob/master/design/completeness_models/shr_completeness_v02.pdf>
* <https://github.com/standardhealth/shr_spec/blob/master/design/completeness_models/shr_completeness_notes_v02.pdf>

## Data-in-Motion Confidentiality [Security, v0]

The HIE site must use TLS/SSL for confidentiality of data while in motion.

## Data-at-Rest Confidentiality [Security, v2]

Any PHI or PII must be kept confidential while at rest (stored) as well. To meet HIPAA requirements, data in motion must be encrypted. Any managed keys used for this encryption will need to be rotated out and replaced once a year.

## Data Integrity [Security, v2]

The accuracy and completeness of data over its lifetime must be ensured by the system. Unauthorized and especially undetected changes to the data must be avoided.

## Distributed Patient Health Records [Patient Record, v3]

A patient’s health record may be physically stored on multiple servers. System should support the logical patient record such that queries can merge results from multiple servers.

System should also support data exchange with the eHealth National Exchange.

## Dynamic Simulated Synthetic Patients [Patient Record, v4]

Later iterations of the synthetic patient feature should simulate the residents of Massachusetts over time and produce birth and death events as well as admit, discharge, and transfer events. Disease surveillance could also be done based on the evolving health records.

## Multiple Patient Lists [Patient Record, v2]

SyntheticMass needs to support the synthetic patient list plus at least one real (and potentially multiple) patient list.

## Non-Repudiation [Security, v2]

Non-repudiation must exist for updates to patient records. If someone updates a patient record, a clear, indisputable audit trail should exist for those updates.

## Patient Matching [Patient Record, v3]

From an e-mail exchange between Harry Sleeper and Andy Gregorowicz:

“I don’t think you are going to get away from some sort of human data quality stewards in the short term. We have heard that organizations will run a fixed patient matching algorithm on their MPI at some fixed interval (say monthly). During that run, the matching algorithm will turn up potential duplicates and the humans will sort them out. As the organization tweaks their patient registration processes, or other data ingest processes, they can see if the number of duplicates trends upward or downward.

Based on that, I would create a KPI of detected duplicates / data exchange. How many duplicates do you create per 1000 CCDA’s you ingest? You could break it down into: How many CCDA (or whatever the data ingest format is) / 1000 require human adjudication? How many out of the human adjudication pool were true duplicates?”

Use Cases Added:

1. 5.12.8 Find Potential Duplicative Patients
2. 5.1.10 Resolve Potential Duplicative Patient Records [Patient Matching, v2]

## PHI Handling / HIPAA Compliance [Patient Record, v2]

1. Put safeguards in place to protect patient health information.
2. Reasonably limit uses and sharing to the minimum necessary to accomplish your intended purpose.
3. Have agreements in place with any service providers that perform covered functions or activities for you. These agreements (BAAs) are to ensure that these services providers (Business Associates) only use and disclose patient health information properly and safeguard it appropriately.
4. Have procedures in place to limit who can access patient health information, and implement a training program for you and your employees about how to protect your patient health information.

Source: <https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html>

A number of other non-functional requirements are covering at least portions of what’s needed for HIPAA compliance although maintaining a separate requirement for HIPAA compliance is important.

## Resilience [Patient Record, v2]

Any security breaches must be limited in scope – minimizing the PHI exposed as much as possible. Perhaps only data currently being processed/accessed (and therefore decrypted) would be at risk. Detecting the breach would be required to avoid access over a long period of time exposing more data.

## Section 508 [Usability, v3]

Section 508 generally requires Federal agencies to ensure that, when developing, procuring, maintaining, or using electronic and information technology, they take into account the needs of all end users – including people with disabilities. Doing so enhances the ability of Federal employees with disabilities to have access to and use of information and data that is comparable to that provided to others. Similarly, agency procurement of accessible EIT enhances the ability of members of the public with disabilities who are seeking information or services from a Federal agency to have access to and use of information and data that is comparable to that provided to others. Comparable access is not required if it would impose an "undue burden" on the agency. If an agency invokes the undue burden exception, the statute requires the information and data to be provided to individuals with disabilities by an alternative means of access. (See section B.6.ii, below). Source: <http://www.section508.gov/content/faq-final#_Toc246911526>

## Static Synthetic Patients [Patient Record, v0]

The system must support a set of synthetic patients representing the 7 million residents of Massachusetts. The patients should be distributed geographically throughout the state per the census data. Each patient should have a complete Standard Heath Record.

## Support Infrastructure [Support, v4]

Need software to log and track the disposition of support requests which may include requested enhancements and defects.

Need a process for disposing of support requests, enhancement requests, and defects. A Change Control Board or some other mechanism for prioritizing items will be required.

# Glossary

## ACO = Accountable Care Organization

An accountable care organization (ACO) is a healthcare organization characterized by a payment and care delivery model that seeks to tie provider reimbursements to quality metrics and reductions in the total cost of care for an assigned population of patients.

## ADT = Admit, Discharge, Transfer

Acronym for three common events for patients – being admitted to a hospital or facility, being discharged from a hospital or facility, and being transferred between medical facilities.

## ARRA = American Recovery and Reinvestment Act

The American Recovery and Reinvestment Act of 2009 is an economic stimulus package. ARRA includes HITECH (see HITECH).

## ASTM = American Society for Testing Materials

Standards organization collaborating on CCD. <https://www.astm.org/>

## Blue Button

As America’s health care system rapidly goes digital, health care providers, insurance companies and others are starting to give patients and consumers access to their health information electronically through the “Blue Button”. [Source: <https://www.healthit.gov/patients-families/faqs/what-blue-button>]

## CCD = Continuity of Care Document

The Continuity of Care Document (CCD) is a joint effort of HL7 International and ASTM. CCD fosters interoperability of clinical data by allowing physicians to send electronic medical information to other health professionals without loss of meaning and enabling improvement of patient care. Source: <http://www.hl7.org/implement/standards/product_brief.cfm?product_id=6>.

## C-CDA (or CCDA) = Consolidated-Clinical Document Architecture

Health Level 7 standard for meeting 2014 Edition EHR Certification Criteria in support of Meaningful Use Stage 2.

## CCDS = Common Clinical Data Set

CCDS is a set of criteria proposed by ONC that includes the required elements for the summary of care document, the standards required for structured data capture of each, and further definition of related terminology and use. Definition: <https://www.healthit.gov/sites/default/files/commonclinicaldataset_ml_11-4-15.pdf>

## CDA = Clinical Document Architecture

The HL7 Clinical Document Architecture (CDA®) is a document markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between healthcare providers and patients. It defines a clinical document as having the following six characteristics: 1) Persistence, 2) Stewardship, 3) Potential for authentication, 4) Context, 5) Wholeness and 6) Human readability. Source: <http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7>

## CDE = Common Data Element

NIH encourages the use of common data elements (CDEs) in clinical research, patient registries, and other human subject research in order to improve data quality and opportunities for comparison and combination of data from multiple studies and with electronic health records. Source: <https://www.nlm.nih.gov/cde/>

## CMS = Centers for Medicare and Medicaid Service

The Centers for Medicare & Medicaid Services, CMS, is part of the Department of Health and Human Services (HHS).

## Covered Function (per HIPAA)

A covered function is any function the performance of which makes the performer a health plan, a health care provider, or a health care clearinghouse.

## CSV = Comma-Separated Values

Format for tabular data in a text file where each record is a line and each cell is separated by commas

## CVX Codes

CVX Codes specify active and inactive vaccines available in the US. See <https://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx>

## Direct

Standard for secure electronic exchange of healthcare information.

## Disease Surveillance

Disease surveillance is an epidemiological practice by which the spread of disease is monitored in order to establish patterns of progression. The main role of disease surveillance is to predict, observe, and minimize the harm caused by outbreak, epidemic, and pandemic situations, as well as increase knowledge about which factors contribute to such circumstances. Source: <https://en.wikipedia.org/wiki/Disease_surveillance>

## DSTU = Draft Standard for Trial Use

Version naming scheme used for FHIR standard. DSTU3 is the latest version which is the Draft Standard for Trial Use 3. See also STU as DSTU3 is being renamed STU3. DSTU/STU releases are precursors to the first official 1.0 release. Source: <http://hapifhir.io/>

## eCQM = Electronic Clinical Quality Measure

eCQMs use data from electronic health records (EHR) and/or health Information technology systems to measure health care quality. The Centers for Medicare and Medicaid Services (CMS) use eCQMs in a variety of quality incentive programs and to publicly report data about quality. Source: [https://ecqi.healthit.gov/**ecqm**](https://ecqi.healthit.gov/ecqm)

## EHR = Electronic Health Record

An electronic health record provides all medical data associated with a patient in an electronic format.

## FHIR = Fast Healthcare Interoperability Resources

Fast Healthcare Interoperability Resources is a draft standard data format for resources that are part of health records and an Application Programming Interface (API) for exchanging those records.

## HAPI-FHIR = HL7 Application Programming Interface FHIR

Open source implementation of the HL7 FHIR specification for Java.

## HIE = Health Information Exchange

Health information exchanges (HIEs) facilitate the secure exchange of health information within and across states. Sharing information in this way is one of the requirements of meaningful use. The Office of the National Coordinator for Health Information Technology (ONC) has made 56 awards totally $548 million to help states and territories in the US develop secure health information exchanges. [Source: <https://www.healthit.gov/patients-families/faqs/what-health-information-exchange>]

## HIPAA = Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 is legislation that provides data security and privacy provisions for medical information.

## HISP = Health Information Service Provider

A Health Information Services Provider (HISP) is an organization that manages security and transport for health information exchange among health care entities or individuals using the Direct standard for transport. There is no specific legal designation for a HISP, nor are HISPs specifically regulated by Meaningful Use certification rules. The term HISP was coined to describe specific message transport functions that need to be performed to support scaled deployment of the Direct standard in the market. HISP functions can be performed by existing organizations (such as EHR vendors or hospitals or HIE organizations) or by standalone organizations specializing in HISP services. Source: <http://geekdoctor.blogspot.com/2014/03/a-primer-on-meaningful-use-and-hisps.html>

## HITECH = Health Information Technology for Economic and Clinical Health

HITECH (part of ARRA) funded HIE development efforts at the state level. It offered incentives to hospitals and health care providers for meaningful use of connected, certified electronic health records. It also offered funding for HIE development.

## HL7 = Health Level 7

Standards organization responsible for FHIR.

## ICD-10 = International Classification of Diseases 10th Edition

ICD-10 is a clinical cataloging system. Within the healthcare industry, providers, coders, IT professionals, insurance carriers, government agencies and others use ICD codes to properly note diseases on health records, track epidemiological trends, and assist in medical reimbursement decisions. Source: <http://searchhealthit.techtarget.com/definition/ICD-10>

## LOINC = Logical Observation Identifiers Names and Codes

See <http://loinc.org/>. LOINC consists of universal identifiers for laboratory and other clinical observations.

## Meaningful Use

Meaningful use is using certified electronic health record (EHR) technology to: Improve quality, safety, efficiency, and reduce health disparities. Engage patients and family. Improve care coordination, and population and public health. Maintain privacy and security of patient health information. Source: <https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives>

## MRN = Medical Record Number

The medical record number is organization specific. The number is used by the hospital as a systematic documentation of a patient´s medical history and care during each hospital stay. Source: <https://ushik.ahrq.gov/ViewItemDetails?system=ps&itemKey=88720000>

## NIH = National Institute of Health

A part of the U.S. Department of Health and Human Services, NIH is the largest biomedical research agency in the world. Source: <https://www.nih.gov/about-nih>

## OAuth2 = Open Standard for Authorization 2

OAuth provides to clients a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. Source: <https://en.wikipedia.org/wiki/OAuth>

## ONC = Office of National Coordinator for Health Information Technology

The Office of the National Coordinator for Health Information Technology (ONC) is at the forefront of the administration’s health IT efforts and is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide health information exchange to improve health care. ONC is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS). Source: <https://www.healthit.gov/newsroom/about-onc>

## OpenID

OpenID is an open standard and decentralized authentication protocol that allows users to be authenticated by co-operating sites (known as Relying Parties or RP) using a third party service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log in to multiple unrelated websites without having to have a separate identity and password for each. Source: <https://en.wikipedia.org/wiki/OpenID>

## PDMP = Prescription Drug Monitoring Program

“Prescription Drug Monitoring Programs (PDMPs) are state-run electronic databases used to track the prescribing and dispensing of controlled prescription drugs to patients. They are designed to monitor this information for suspected abuse or diversion (i.e., channeling drugs into illegal use), and can give a prescriber or pharmacist critical information regarding a patient’s controlled substance prescription history. This information can help prescribers and pharmacists identify patients at high-risk who would benefit from early interventions.” Source: <http://www.cdc.gov/drugoverdose/pdmp/>

## PHI = Protected Health Information

Information in a medical record that identifies an individual created in the process of providing health care (e.g., a diagnosis or treatment).

## PII = Personally identifiable information

Personally identifiable information (PII) as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Source: <https://en.wikipedia.org/wiki/Personally_identifiable_information>

## QRDA = Quality Reporting Document Architecture

The Health Level Seven International (HL7) Quality Reporting Document Architecture (QRDA) is a standard document format for the exchange of electronic clinical quality measure (eCQM) data. Source: <http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35>

## RxNORM

RxNorm provides normalized names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software. Source: <https://www.nlm.nih.gov/research/umls/rxnorm/>

## SFTP = Secure (or SSH) File Transfer Protocol

Internet standard protocol for transferring files securely. SSH encryption provides confidentiality and integrity of data transported over an unsecure network.

## SHR = Standard Health Record

MITRE’s vision is to ***fundamentally shift*** how healthcare providers and individuals obtain and use pertinent information across multiple care domains to manage acute and preventive health. This shift begins with defining a Standard Health Record (SHR) to address the US healthcare system’s critical need for health data interoperability. The SHR vision is to enable unfettered multi-directional communication, driven by real-time, meaningful data, that empowers individuals and care teams to collaborate, reduce error and waste, and focus on the shared-decision making needed to build and maintain a healthy nation. Source: SHR Overview\_v3\_7\_25\_16.docx by Mary Quilty

## SMART on FHIR

SMART on FHIR is a platform to enable medical applications to be written once and run unmodified across different healthcare IT systems. SMART on FHIR was developed by a project started in early 2010 by Harvard Medical School and Boston Children’s Hospital.

A SMART on a FHIR system is a health IT system that has implemented the SMART on a FHIR specification, including our profiled versions of FHIR, OAuth2, and OpenID Connect. Such a system is capable of running SMART apps. Source: <http://jamia.oxfordjournals.org/content/early/2016/02/16/jamia.ocv189>

## SNOMED = Systematized Nomenclature of Medicine

The Systematized Nomenclature of Medicine is a systematic, computer-processable collection of medical terms, in human and veterinary medicine, to provide codes, terms, synonyms and definitions which cover anatomy, diseases, findings, procedures, microorganisms, substances, etc. The standard is now more specifically called SNOMED-CT where CT stands for Clinical Terms. Source: <https://en.wikipedia.org/wiki/Systematized_Nomenclature_of_Medicine>

## SSH = Secure Shell

SSH is a secure network protocol for operating network services over an unsecured network.

## STU = Standard for Trial Use

Current naming convention for releases of FHIR standard. STU3 is the latest release as of July 2016. Source: <http://hapifhir.io/>

## XDM = Cross-Enterprise Document Media Interchange

Cross-Enterprise Document Media Interchange (XDM) provides document interchange using a common file and directory structure over several standard media types. XDM is used as part of Direct. Source: <http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol1_FT_2010-08-10.pdf#page=128>

## XDR = Cross-enterprise Document Reliable Interchange

XDR provides document 480 interchange using a reliable messaging system. This permits direct document interchange between EHRs, PHRs, and other healthcare IT systems in the absence of a document sharing infrastructure such as XDS. XDR is used as part of Direct. Source: <http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol1_FT_2010-08-10.pdf#page=128>

# Appendix A – Multiple Patient Repositories

In order to support all use cases on a common server instance, we need to separate out synthetic patients and real patients (See 6.1 Support Multiple Patient Lists). Potentially, support for multiple, separate, secure patient repositories may be needed as well.

**Option 1**: FHIR does offer a compartment concept that can be named and has a boolean attribute labelled “experimental” that indicates the compartment definition is authored for testing purposes. It also includes a publisher such that the synthetic data can be attributed to MITRE Synthea. It also includes a requirements attribute that can be used to describe the scope and usage that the compartment definition was created to meet. Predefined compartment types are focused around isolating the data for a particular resource (e.g., a single patient), but potentially it could be used for a list of patients and their associated data as well? Example of using a compartment in a search:

GET [base]/[Compartment]/[id]/[type]{?[parameters]{&\_format=[mime-type]}}

See <http://hl7.org/fhir/2016May/compartmentdefinition.html> and <http://hl7.org/fhir/2016May/http.html#vsearch>.

**Option 2**: Use Organization as the separator between patient lists. The synthetic patients can also be listed under “SyntheticMass” as an organization for example.

**Option 3**: Of course, multiple FHIR service instances with separate databases could be used as well. The web application would then need to support multiple FHIR endpoints.