Grant Final Report

Grant ID: 1UC1HS015220

SAFEHealth: Secure Architecture for Exchanging Health Information

Inclusive Dates: 09/30/04 - 09/29/09

Principal Investigator:
Lawrence David Garber, MD

Team Members:

Peggy Preusse, RN	Chris Diguette
Diane Gannon, RN	Devi Sundaresan
Giancarlo Vivenzio	Ellen Trencher
James Underwood	Val W. Slayton, MD, MPP, MBA

Performing Organization:
Fallon Clinic
Worcester, Massachusetts

Project Officer:
Jayasree (Joy) Basu

Submitted to:
The Agency for Healthcare Research and Quality (AHRQ)
U.S. Department of Health and Human Services
540 Gaither Road
Rockville, MD 20850
www.ahrq.gov

Abstract

Purpose: Build, operate and evaluate SAFEHealth, a health information exchange (HIE) designed to enable secure, real time transfer of patients' health information between organizations with patient consent to improve the quality, safety and efficiency of healthcare.

Scope: This scalable HIE was constructed in Massachusetts to exchange clinical data between a large group practice and an acute care hospital with patient consent.

Methods: Patient and physician focus groups provided feedback on HIEs. Functional requirements for the HIE were defined and software was developed. Policies, procedures, and consent forms were created to support the HIE which became functional in June 2009. Participants were surveyed regarding the impact of SAFEHealth.

Results: Patient focus groups supported SAFEHealth with "Opt-In" consent. Physician focus groups also supported SAFEHealth, but revealed concerns about information overload and liability. A federated edge-proxy server HIE with an EMPI was implemented. Clinical data was transferred from EHR to EHR. After 15 weeks of use, 750 patients had consented and approximately 6000 clinical documents had been exchanged. Overall, participants felt the HIE was valuable. SAFEHealth is financially sustainable due to high value and low operating expenses.

Key Words: Health Information Exchange, HIE, RHIO, federated, patient consent, authorization, privacy, security, sustainability, quality, safety, efficiency

The authors of this report are responsible for its content. Statements in the report should not be construed as endorsement by the Agency for Healthcare Research and Quality or the U.S. Department of Health and Human Services of a particular drug, device, test, treatment, or other clinical service.

Final Report

Purpose

The goal of this study was to implement and evaluate a financially sustainable health information exchange (HIE) that would improve patient safety, quality of care, and efficiency of healthcare delivery, and elucidate how others could do this most efficiently in the future. The objectives of this study involved evaluating the entire implementation of an HIE known as SAFEHealth - **S**ecure **A**rchitecture **F**or **E**xchanging Health Information, that was capable of secure, real time transfer of patients' health information between multiple different organizations with patient consent. This evaluation would involve all of the steps, including stakeholder participation, defining functional requirements, obtaining funding, developing and implementing the HIE, assessing its financial sustainability, and evaluating its impact.

Scope

Traditionally, healthcare delivery has been a complex and poorly coordinated system that involves clinical information being generated at numerous different physical locations and poor communication between those locations. Indeed, the average Medicare patient sees approximately 7 different physicians each year. Patients often become the communication medium between healthcare providers, but they often produce inaccurate verbal accounts of this clinical information. This inadequate communication results in treatment decisions based upon incomplete and/or inaccurate information, redundant testing in an attempt to fill the information voids, and the potential for healthcare quality and safety issues. This problem is particularly evident as patients transition between care settings. For instance in one study, the treating physician was lacking important medical information in 30% of Emergency Department visits, half of which were deemed "critical."[1] Similarly, there are approximately 2 million preventable adverse events each year due to inadequate communication at the time of hospital discharge.[2] It has been estimated that almost 20% of preventable medical errors are due to inadequate availability of patient information at the point of care.[3]

To help solve these problems, Community Health Information Networks (CHINs) were formed in the early 1990s. These were large databases where clinical information was gathered from multiple different sources and organizations. However most of these failed because of lacking a financially sustainable model, as well as concerns about storing clinical information in a central location where ownership of the data is unclear. To mitigate these concerns, in the early 2000s, Fallon Clinic among others recognized that the clinical data could be stored by the organizations that care for each specific patient. By placing "edge proxy" servers that would cache copies of patient data in a distributed, federated architecture behind each organization's firewall, these servers could coordinate the secure transfer of patient clinical information to other organization when appropriate.

Controlling the flow of this clinical information quickly became the next logistical problem. While HIPAA Privacy and Security regulations allow for the transfer of clinical information based on the Notice of Privacy for the purpose of treatment, payment, and operations, many states have laws that supersede HIPAA. For instance in Massachusetts, patients need to sign separate consents to release HIV and mental health-related information. This leads to the dilemma of choosing between filtering out this particularly sensitive information (which might result in patient safety issues and is arguably impossible to accomplish anyway), or obtaining "Opt-In" consents from patients (which might require modifying EHRs and could interfere with workflows in busy Emergency Departments).

In order to tackle these issues, Fallon Clinic partnered with UMass Memorial Healthcare System and Fallon Community Health Plan to create a functional, scalable and sustainable HIE know as SAFEHealth- **S**ecure **A**rchitecture **F**or **E**xchanging Health Information. Two models were implemented. One using patient "Opt-In" consent was built to interconnect Fallon Clinic's EHR (Epic) with HealthAlliance Hospital's Leominster Campus Emergency Department EHR (Siemens). The other was based on the HIPAA Notice of Privacy to push the "results" from Milford Regional Medical Center care (MEDITECH) back to the Fallon Clinic referring physician.

Fallon Clinic is a large not-for-profit multi-specialty group practice with more than 20 locations throughout Central Massachusetts. Fallon Clinic has over 1,700 employees and approximately 250 physicians representing over 30 specialties. UMass Memorial Health Care's HealthAlliance Hospital is a not-for-profit, full service, acute care hospital that serves the communities of North Central Massachusetts. Milford Regional Medical Center is a 121-bed, nonprofit, acute-care facility serving South Central Massachusetts.

Methods

Six patient focus groups and two physician focus groups were convened with a professional moderator, videotaped and scored to gather feedback on HIEs. The patient focus groups were segregated into the following types: Chronically Ill, Acutely Ill, Caregivers and Healthy adults. The physician focus groups were divided into two categories: Primary Care, consisting of internists and pediatricians; and Specialists including a cardiologist, obstetrician, neurologist, rheumatologist and a pulmonologist.

Functional requirements for the HIE were defined based on the findings from the focus groups, stakeholder interviews, and extensive literature review. Software was then developed to meet these specifications. This software development was initially attempted through an elaborate process of renting office and data center space, hiring several programmers, purchasing site licenses for software development tools, and creating a formal Regional Health Information Organization (RHIO). After realizing that this approach was too expensive, we attempted to find a software development partner. However after several attempts we could not find a software development firm that truly wanted to be a partner. As a result, we scaled down the software development activity to involve just Fallon Clinic's IT staff, taking advantage of shared fixed costs. The participating organizations agreed to share in the development and implementation costs, including providing resources for testing the software.

Workgroups were created to define data standards and to develop policies and procedures regarding data ownership/use and privacy/security. Universal consent and revocation of authorization forms were created and approved by the participating organizations (see Appendices A and B).

Registration staff each received 30 minutes of training just before go-live using a hands-on computer lab classroom environment. While physicians and nurses received no formal training because clinical data from SAFEHealth appears within the EHR that they had separately been taught to use, Dr. Garber presented a hospital Grand Rounds to provide general education on HIEs.

Patients received general education through the SAFEHealth.org website, newspaper articles and advertisements, as well as posters in the waiting rooms. They also received individual education by the registration clerks obtaining consent as well as from pre-printed brochures.

SAFEHealth became fully operational on June 24th, 2009 using a federated edge-proxy server architecture with patient "Opt-In" for clinical data exchange managed by a consent engine external to the EHR. A central Enterprise Master Person Index (EMPI) was pre-loaded with the demographic information (name, gender, date of birth, and zip code) from 1 million patients. HealthAlliance Hospital's Leominster Campus Emergency Department provided ER notes while Fallon Clinic provided two years of historical notes, including medication lists, allergies, problem lists, immunizations, code/advanced directive status, vital signs, recent lab/radiology results, and the Primary Care Physician's name and phone number. Clinical data was imported directly into the receiving organization's EHR for use during treatment. Physicians and staff were subsequently surveyed in December 2009 regarding the impact of SAFEHealth.

Separately, a one-way interface was established from the Milford Regional Medical Center's EHR into Fallon Clinic's EHR on July 1st, 2009. Textual imaging/test/procedure/visit/discharge reports are transmitted if the patient was under the care of a Fallon Clinic physician or had a Fallon Clinic referring physician. Physicians were subsequently surveyed in December 2009 regarding the impact of the interface.

Results

Patient focus groups revealed that patients overwhelmingly thought the benefit of health information exchange outweighed any security risk, but formal consent should be obtained from each patient (i.e. "Opt-In") prior the exchange of any clinical data. Physician focus groups revealed concerns about information overload and liability, but that overall they rated the SAFEHealth concept highly.

Based on the findings from the focus groups, stakeholder interviews and extensive literature review, ten high-level design goals were identified which drove the development and implementation of SAFEHealth:

- One central demographic repository/Enterprise Master Person Index (EMPI)

- No central clinical data repository

- Patients “Opt-In” once at the connected entity/organization level for all data content/types for Treatment/Payment/Operations uses only. Patients can revoke access to any or all entities at any time. Patients only have to go to one entity/organization in order to execute all of their authorizations and revocations.
- All authorized entities/organizations can access the entire patient record
- Clinical data flows from EHR to EHR, and is viewed by clinicians directly within their EHRs
- User authentication and role-based access is performed by each connected entity through their EHR
- Minimize duplicate data from multiple sources
- Scalable and high performance
- No rip and replace – leveraging existing systems with minimal modification
- Integrate seamlessly into physician & staff workflows

The result was a federated, edge-proxy server architecture with patient “Opt-In” for clinical data exchange managed by a consent engine external to the EHR. The software was written in Microsoft .NET and uses MS SQL Server 2005. Each edge proxy server contains a TP13/XDS.b-like Document Repository and Document Registry. As data flows from the EHR into the local Document Repository, it is transformed by SAFEHealth’s interface engine into standard terminologies including SNOMED-CT, LOINC, and NPI numbers.

Access control is managed through an SC108/BPPC-like Consent Portal/Repository. As patients are “arrived” for their visits, the SAFEHealth Consent Portal/Repository monitors the EHR’s ADT interface, checks to see if the patient needs to sign a SAFEHealth Universal Consent Form and if so, prints it out on the printer closest to the registration clerk. Consent is to authorize a participating entity to both disclose as well as to receive all patient information, including sensitive info (e.g. HIV, STDs, Mental Health, Genetic testing, etc…). Patients can authorize any or all of the current entities participating in SAFEHealth, or they can authorize any current or future healthcare provider in the entire state of Massachusetts in case they were to seek care there. Patients can also authorize their medical insurance carrier(s) to provide claims information to SAFEHealth. Consent only needs to be signed once at one organization to authorize any or all entities. Authorizations are forever; however, consent can be revoked by a patient at any time for any or all entities for future disclosures and viewing, but past disclosures cannot be revoked. When a parent or guardian consents for a minor, an expiration date of their 18th birthday is automatically entered into the consent record.

After the consent form is signed, the registration clerk clicks next to patient’s name in the work list of the Consent Portal to acknowledge that the form was or was not signed and which entities were authorized, triggering clinical data to be exchanged between these authorized entities and allowing import into the local EHRs. This SAFEHealth consent process can be done asynchronously with standard registration/check-in workflows so it doesn’t interfere with patient care, even in busy Emergency Departments. Patients who do not consent to all current participating providers will not have a consent printed for another year so as not to annoy someone who truly doesn't want to participate. Of course, patients can visit any participating organization at any time to have a consent or revocation form manually printed and entered.

Authorized organizations continuously have new clinical information from other authorized organizations pushed to them, and can have this information uploaded into their local EHR for up to 1 year from the last patient encounter in that organization (e.g. for handling telephone calls from the patient). Clinical information after 1 year from the last visit is "held" without EHR upload. However if after that time, the patient is seen again, any "held" clinical information is automatically uploaded into the local EHR when the patient arrives for a visit.

A central EMPI was pre-loaded with the demographic data (name, gender, date of birth, and zip code) from approximately 1 million patients. This central collection of patient demographic data was necessary for efficient and consistently accurate patient matching between organizations and enables a universal consent to be signed at any organization without having to be signed at each individual organization. The EMPI was internally developed using Microsoft .NET and MS SQL Server 2005. It uses name (first, middle, last), gender, date of birth, and zip code for probabilistic matching purposes. Prior to matching, the EMPI normalizes names for variations in data entry at different organizations (e.g. "St. Denis", "St Denis" and "StDenis" are all recognized as being the same). It has flexibility in terms of how middle names match and accommodates aliases and gender changes. It also takes into account the geographic proximity of addresses.

After the first 15 weeks of use, 750 patients had signed consents to participate in SAFEHealth and 2 people had revoked their consent. Approximately 50% of patients consented to share all of their records with any healthcare organization in Massachusetts that cares for them, and 70% agreed to allow information from their health insurer to be shared with their healthcare providers. Approximate 6000 clinical documents had been exchanged during these first 15 weeks. However, less that 50% of patients who were offered to participate in SAFEHealth actually signed the consent form. Interviews with the registration clerks gave clues as to the reason for this low consent rate compared to the ~95% consent rate seen in the Massachusetts eHealth Collaborative (MAeHC) communities. Currently, only 2 organizations are connected to SAFEHealth. As a result, many patients said that they would never be going to other organization for care so they didn't see a need to participate. If more of their healthcare provides were participating, many more would likely have consented.

Physicians and staff were surveyed in December 2009 regarding the impact of SAFEHealth. As mentioned above, the registration clerks confirmed that many patients perceived their care as only being with one organization and not involving others. As a result they didn't see the need to participate in SAFEHealth. This suggests the need for not only the expansion of SAFEHealth to other organizations that patients may seek care from, but also more generalized marketing of the HIE concept and its benefits. We know from the focus groups described earlier, that patients are receptive when properly educated about HIEs. In the focus groups, patients received 20-30 minutes education about HIEs, whereas during the registration process, the education is less than 1 minute. Yet overall, even in a busy Emergency Department, the registration clerks were very positive about the workflow for obtaining and entering patient authorizations for SAFEHealth.

Physicians overall found SAFEHealth valuable, however they did identify room for improvement. While finding information in their EHR was more convenient than having to call for records or going to a separate website, they still felt that having access to information filed more discretely (e.g. lab results in the lab section) would be even better. This is certainly possible with the SAFEHealth architecture, but due to time constraints we did not get to mapping lab and other test results. Instead, these were merged into the corresponding visit notes which made them harder to find.

The financial sustainability of SAFEHealth is a concern that is common to all HIEs. One approach when establishing a HIE is to create a formal RHIO, build data centers, buy commercial software, hire staff, and then charge huge subscription fees to pay for the tremendous operating expenses of such an organization. We started down a similar path early in our project. In the first 3 years of this project we spent $4.5 Million and for the most part only had policies, procedures and lessons learned. We learned that a group of healthcare organizations can collaborate under existing state and federal laws without the need to make a formal RHIO, saving a great deal in legal expenses. Similarly you can develop software internally within a good IT shop which can leverage existing software licenses and data centers. In the end, SAFEHealth was developed and implemented in less than 2 years for approximately $1 Million. And the beauty of this relatively low-cost, internally-developed software approach is that it results in extraordinarily low operating expenses going forward. SAFEHealth will be financially sustainable by having each organization paying for their own expenses (MS SQL Server License and server maintenance contract) which is approximately $2,000 (two thousand dollars) per year per organization with current functionality.

A similar approach to sustainability was used with the one-way interface that was established from the Milford Regional Medical Center's EHR into Fallon Clinic's EHR on July 1st, 2009. Using this T31/XDR-like interface, approximately 10,000 clinical documents have been transferred in the first 15 weeks since the system went live. Yet the cost to maintain this interface for each connected organization is merely a few hundred dollars/year.

Physicians were surveyed in December 2009 regarding the impact of the Milford Regional Medical Center's interface. This interface filed test results and notes more discretely into appropriate section of the EHR than was done with the SAFEHealth interface. So as anticipated from the SAFEHealth physician survey results, the users of the Milford Regional Medical Center's interface were even more satisfied with their ability to find information. In fact, *all* of the physicians felt *strongly* that they were able to provide higher quality, safer medical care more efficiently and effectively as a result of this interface.

Conclusions

This 5-year journey to create a functional and financially viable Health Information Exchange was really divided into the first 3 years where multiple difficult lessons were learned, followed by 2 years of highly productive and rewarding work. It is our hope that others will learn from our experiences and be able to jump right to those productive years.

Everyone agrees that the key to a financially sustainable HIE is to provide value to each stakeholder such that they can justify paying for that value. We further believe that the key to hitting a price-point that stakeholders will fund is to dramatically lower operational expenses. As such, we enabled low operating expenses ($2,000/organization/year) by:

- Internally-developing the software using existing IT staff and tools

- Hosting the central server in one of our trusted organizations' data center

- No formal third-party organization/RHIO

We found that point-to-point T31/XDR-like interfaces work very well to push clinical data to the ordering or referring physician. These transactions did not require explicit patient consent as they are covered under the HIPAA Notice of Privacy.

Similarly, we found that a federated, edge proxy server containing a TP13/XDS.b-like Document Repository and Document Registry could be used effectively to synchronize clinical content between multiple authorized healthcare organizations.

We also found that in Massachusetts, where explicit consent needs to be signed in order to release HIV or Mental Health information on patients, an all-or-nothing “Opt-In” consent model is required. We do not believe that such specially-protected information buried in textual notes or implied by medication lists, allergy lists, or test results will ever allow for reliable filtering of clinical information. Even if it were possible, we believe that it would be dangerous for patients as they cannot realize the implications of not conveying such medical history. Similarly we don’t believe that information can practically be limited to one practitioner within an organization that uses a shared EHR. Indeed, very few EHR users attempt to use “hard-stops” to prevent such access. Instead, other measures such as audit trails and legal action against inappropriate use are used as deterrents. As such, there is a rapidly growing divide between patient expectations for controlling their clinical data, and what is technologically possible.

Lastly, we found that integrating a HIE into the real-life healthcare workflows of patients, registration clerks, and physicians is a critical success factor. By using a central EMPI and an SC108/BPPC-like Consent Portal/Repository outside of the EHR, we were able to allow patients to a sign a single universal consent form that declared which specific organizations could exchange their data. By printing the consent form automatically only when needed, registration clerks did not have to go out of their way in order to figure out whether a consent was needed. Furthermore, the Consent Web Portal made it easy for the registration clerk to enter the resulting consent information literally with one click directly into a work list of printed consents.

Similarly physicians did not need to wonder about whether outside data existed on their patients; they were simply able to see this as part of their normal workflows using their own EHR. They didn’t need to learn new systems or obtain new passwords. In fact, they received no formal training whatsoever and were able to immediately access the SAFEHealth data. They did, however, identify that filing data more discretely into appropriate sections of the EHR (e.g. lab, imaging, etc...) would make it even easier to find relevant information in a timely manner. This was proven through our interface with Milford Regional Medical Center which filed test results and notes more discretely into appropriate section of the EHR than was done with the SAFEHealth interface because of the additional effort placed in mapping. As a result, *all* of the physicians felt strongly that they were able to provide higher quality, safer medical care more efficiently and effectively as a result of this more fully-mapped interface.

We are somewhat disappointed that the patient consent rate was not as high as others have found, but feel that as more organizations are added to SAFEHealth and more general education about HIEs becomes ubiquitous, patients will see more value in SAFEHealth and be more willing to consent to participate.

In summary, the SAFEHealth’s internally-developed federated, edge proxy server architecture with central Enterprise Master Person Index (EMPI) and a Consent Portal/Repository external to the EHR filing data discretely into each EHR, is a formula for a successful and financially sustainable Health Information Exchange (HIE).

Inclusion of AHRQ Priority Populations

This project allows any patient to participate in SAFEHealth, therefore we equally include and represent the rights of AHRQ's priority populations, including women, children, elderly, minorities, inner-city, rural, low income, chronically ill and the disabled.

We would like to take this opportunity to thank the Agency for Healthcare Research and Quality (AHRQ) for their support of SAFEHealth and the healthcare community of Central Massachusetts through this grant. We will continue to look for opportunities to show how SAFEHealth has impacted our community and disseminate lessons learned to others.

References

1. Stiell A, Forster AJ, Stiell IG, van Walraven C. Prevalence of information gaps in the emergency department and the effect on patient outcomes. CMAJ. 2003 Nov 11;169(10):1023-8.

2. Forster AJ, Murff HJ, Peterson JF, Gandhi TK, Bates DW. The Incidence and Severity of Adverse Events Affecting Patients after Discharge from the Hospital. Annals of Internal Medicine 138: 161-167. 2003.

3. Kaelber DC, Bates DW. Health information exchange and patient safety. J Biomed Inform. 2007 Dec;40(6 Suppl):S40-5. Epub 2007 Sep 7.

List of Publications and Products

While no formal publications have been generated to date as a result of this grant, we have made multiple presentations disseminating our lessons learned. Two of these are available on the SAFEHealth.org website:

Garber LD. SAFEHealth – Architecture, Workflows and Policies. Massachusetts Health Data Consortium CIO Forum; 2009 Nov 18. http://www.safehealth.org/about/SAFEHealth%20Presentation%20to%20MHDC%20CIO%20Forum%20-%20November%2018,%202009.ppt

Garber LD. SAFEHealth - A Public Utility for Electronically Exchanging Clinical Information in Central Massachusetts. HealthAlliance Hospital Grand Rounds; 2009 Mar 3. http://www.safehealth.org/physicians/Health%20Alliance%20Hospital%20Grand%20Rounds%20-%20SAFEHealth.ppt

Appendixes

Appendix A: Universal SAFEHealth Consent Form

SAFEHealth

Consent for Health Information Exchange

1. **Patient Information**

Name:____

Date of Birth:_________ Phone #:__________________ Alternate Phone #:___________________

Street:____

City:___________________________________ State:____________ Zip:______________________

2. **Authorization to Participate in SAFE Health**

I authorize my medical providers to **RELEASE/SHARE/DISCLOSE** and **VIEW all of my electronic health record information** through the secure SAFE Health network with other healthcare providers involved in my care that participate in the SAFE Health network **for the purpose of providing me with medical care**. The participating health care entities that I specifically authorize will be able to see my electronic health record in order to help **make higher quality and safer medical decisions** that will be based on a more complete picture of my medical history. My electronic health record cannot be changed by other participating healthcare institutions. I understand that I can give similar consent at the other healthcare institutions participating in the SAFE Health network.

My electronic health record contains notes from my doctors and other medical providers about my overall health and illnesses that I have had, including diagnoses, physical findings, medications and allergy lists as well as test results such as lab and radiology reports. Although substance abuse and behavioral health records are generally kept separately by mental health providers at their own facility, my other medical record notes may include some **SENSITIVE** information relating to behavioral health and or substance abuse issues, and the medications given to treat these conditions. These notes might also include **SENSITIVE** information regarding sexually transmitted diseases, acquired immunodeficiency syndrome (AIDS) or Human Immunodeficiency Virus (HIV) as these conditions are part of the overall health picture and may require specific medications and treatment. Specifically, my electronic health record may include notes, diagnoses, test results, and medications regarding HIV/AIDS, sexually transmitted disease, alcoholism/alcohol use, drug dependency, addiction or abuse, pregnancy, abortion or family planning, illegitimacy of birth, genetic diseases or predispositions, mental illness or retardation, domestic violence, as well as communications between clinicians and social workers, psychotherapists, psychologists, family or marriage counselors or other mental health advisors that could be sensitive.

I understand that for my convenience, and for the potential to enhance my medical care, this consent permits each entity that I authorize below to release/share/disclose my electronic health record to other healthcare professionals participating in my health care via the secure SAFE Health network. This will allow copies of notes, test results and other health information to be sent through the SAFE Health network to physicians involved in my health care who are part of one of the other SAFE Health participating healthcare entities that I authorize. This consent also permits each participating healthcare entity that I authorize below to view my electronic health record information via the SAFE Health network as part of my medical care.

With a signature below, I can also authorize my medical insurance carrier(s) to provide diagnoses, procedures and medication history to my healthcare providers. This authorization does **not** permit my medical insurance carrier(s) to view any of my medical information via the SAFE Health network.

Unless I request otherwise as described below, this consent will not expire.

I also realize that the transmission of some of my health information via the SAFE Health network may occur independent of this written consent, such as the results of tests or referrals sent to the ordering physician. I understand that these transmissions have traditionally taken place without SAFE Health as part of standard health care business practices authorized by State and Federal regulations, and these industry standard practices will continue even if I do not consent for participation in SAFE Health.

3. Authorization to Participating Entities in the SAFE Health Network

I authorize the following entities to release/share/disclose and view my electronic health information **if and when I seek care**, except for my medical insurance carrier which will **not** be able to view my health information via SAFE Health. I can authorize each entity with an individual signature, or authorize all current SAFE Health participants with a single signature. Alternatively, in order to avoid the need to sign this authorization again as the SAFE Health network adds more of my healthcare providers in the future, I can authorize any current and future healthcare provider in Massachusetts to release/share/disclose and view my electronic health information **if and when I seek care**.

- HealthAlliance Hospital Signature ____________________________ Date ___/___/___
- Fallon Clinic Signature____________________________ Date ___/___/___
- Saint Vincent Hospital Signature ____________________________ Date ___/___/___
- My medical insurance carriers (**disclose only**) Signature ____________________________ Date ___/___/___

------- **OR** -------

- All of the above entities ____________________________ Date ___/___/___
  Signature

------- **OR** -------

- All current and future Massachusetts healthcare providers **and disclosure only** from my medical insurance carriers ___________________________ Date ___/___/___
  Signature

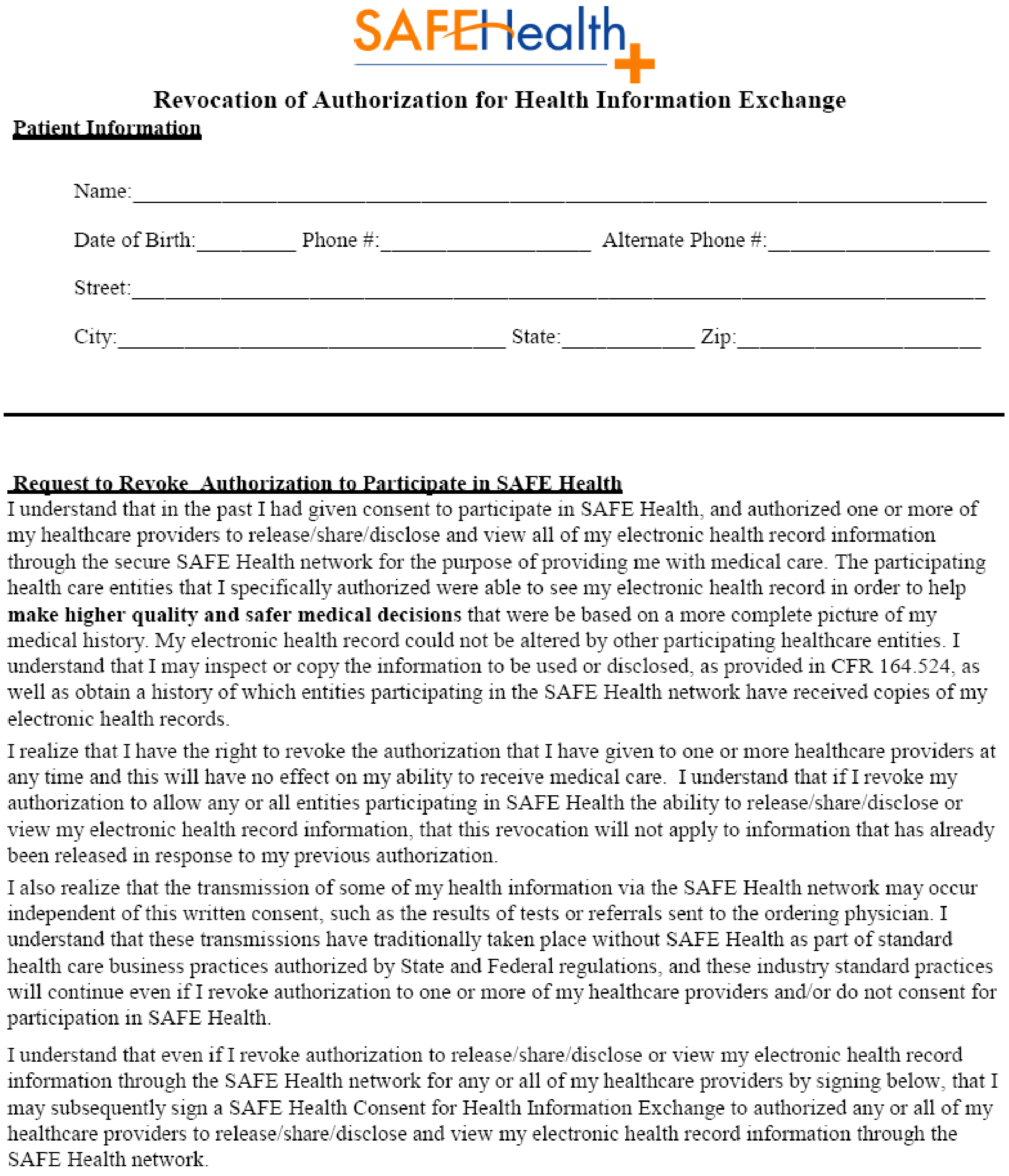
4. Informed Consent

I understand that I have a right to revoke this authorization at any time. I understand that if I revoke my authorization to allow any or all entities participating in SAFE Health the ability to release/share/disclose or view my electronic health record information, I must do so in writing and present my written revocation to a medical provider at any one of the entities participating in SAFE Health. I understand that the revocation will not apply to information that has already been released in response to this authorization. I also understand that, should more entities join the SAFE Health network after I sign this authorization, I would need to give my consent to each new entity prior to any of my protected health information being released/shared/disclosed or viewed by those new entities, unless I authorized all Massachusetts healthcare providers by signing above.
I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this authorization. Refusing to sign authorization will in no way impact my ability to seek medical care at any SAFE Health participating entity. I need not sign this form in order to assure treatment. I understand that I may inspect or copy the information to be used or disclosed, as provided in CFR 164.524, as well as obtain a history of which entities participating in the SAFE Health network have received copies of my electronic health records. I understand that any disclosure of information carries with it the potential for an unauthorized redisclosure and the information may not be protected by federal confidentiality rules.

If I have questions about disclosure of my health information, I can contact the Fallon Clinic Medical Records Department at 1-800-635-1221 or the HealthAlliance Hospital Leominster Campus at 978-466-2805. I may request a copy of this authorization. I understand and agree to all of the information in this authorization document.

____	______________________________
Signature of Patient or Legal Representative	Date signed
____	______________________________
Printed name & relationship to Patient (if signed by Legal Representative)	Signature of Witness

Appendix B: Universal SAFEHealth Authorization Revocation Form



SAFEHealth

Revocation of Authorization for Health Information Exchange

Patient Information

Name:____

Date of Birth:_________ Phone #:___________________ Alternate Phone #:____________________

Street:____

City:___________________________________ State:____________ Zip:______________________

Request to Revoke Authorization to Participate in SAFE Health

I understand that in the past I had given consent to participate in SAFE Health, and authorized one or more of my healthcare providers to release/share/disclose and view all of my electronic health record information through the secure SAFE Health network for the purpose of providing me with medical care. The participating health care entities that I specifically authorized were able to see my electronic health record in order to help **make higher quality and safer medical decisions** that were be based on a more complete picture of my medical history. My electronic health record could not be altered by other participating healthcare entities. I understand that I may inspect or copy the information to be used or disclosed, as provided in CFR 164.524, as well as obtain a history of which entities participating in the SAFE Health network have received copies of my electronic health records.

I realize that I have the right to revoke the authorization that I have given to one or more healthcare providers at any time and this will have no effect on my ability to receive medical care. I understand that if I revoke my authorization to allow any or all entities participating in SAFE Health the ability to release/share/disclose or view my electronic health record information, that this revocation will not apply to information that has already been released in response to my previous authorization.

I also realize that the transmission of some of my health information via the SAFE Health network may occur independent of this written consent, such as the results of tests or referrals sent to the ordering physician. I understand that these transmissions have traditionally taken place without SAFE Health as part of standard health care business practices authorized by State and Federal regulations, and these industry standard practices will continue even if I revoke authorization to one or more of my healthcare providers and/or do not consent for participation in SAFE Health.

I understand that even if I revoke authorization to release/share/disclose or view my electronic health record information through the SAFE Health network for any or all of my healthcare providers by signing below, that I may subsequently sign a SAFE Health Consent for Health Information Exchange to authorized any or all of my healthcare providers to release/share/disclose and view my electronic health record information through the SAFE Health network.

<u>Revocation of Authorization to Participating Entities in the SAFE Health Network</u>

I no longer authorize the following entities with my adjacent signature, to release/share/disclose or view my electronic health record information through the SAFE Health network, excluding that which is part of normal health care operations and standard business practices allowable by State and Federal regulations.

- HealthAlliance Hospital Signature ____________________________ Date ___/___/___
- Fallon Clinic Signature ____________________________ Date ___/___/___
- Saint Vincent Hospital Signature ____________________________ Date ___/___/___
- My medical insurance carriers Signature ____________________________ Date ___/___/___

------- **OR** -------

- I no longer wish to participate in SAFE Health ____________________________ Date ___/___/___
  Signature

____ ______________________________

Printed name & Relationship to Patient Signature of Witness
(if signed by Legal Representative)