Designing a Secure Blue Button Health Information Exchange for a Commercial Laboratory

Seth Baker, Alex Roman
Connected Health Symposium 2015
www.iproc.org/2015/1/e7
DOI: http://doi.org/10.2196/iproc.4685

Abstract

Background: There is a growing demand by patients for easy electronic access to laboratory result data for use in personal health record systems (PHR-S) and for transfer to other health providers. The Blue Button Initiative is a public-private partnership offering a framework based on national standards to support patient access to electronic data.

Objective: The aim of this project study was to architect an initial pilot implementation of the Blue Button framework for a commercial laboratory to facilitate patient access to electronic results.

Methods: The proposed design architecture includes multiple application services, specifically an Encrypted Data Store, Client Access component, and Result Publishing service to accomplish these goals of the pilot project and meet the security and privacy requirements.

Results: The resulting application components and programming interfaces accomplish the initial pilot goals and provide a base to expand the platform to offer support for mobile devices and additional interoperability options. Encryption and isolation of data have been used to safeguard the confidentiality, integrity and availability of protected health information (PHI) and allow for the use of standard cloud services to host external facing components.

Conclusions: The Blue Button standards and framework provide a solid basis for facilitating electronic access to result data by patients and for meeting the requirements of View, Download, and Transmit (V/D/T) in Meaningful Use Stage 2 (MU-II).


**Introduction**

Health information exchange (HIE) is vital to improving health care quality, safety, and patient outcomes. Within the United States, there is growing recognition that healthcare must become more cohesive to achieve the “Triple Aim” goals of improved health outcomes, enhanced patient experience and reduced healthcare costs\(^1\). In an international study on healthcare systems, the USA ranked last in care coordination with 33% of patients reporting that records were not available for an appointment with a doctor or that a doctor ordered an unnecessary medical test that had already been done\(^2\). The Blue Button framework is both a HIE methodology and a symbol of a movement towards an improved healthcare system in which patients and healthcare providers use information technology to work together and improve health\(^3,4,5\).

Blue Button is a registered service mark of the US Department of Health and Human Services and is most often indicated by a clickable blue circle often marked with the text "Download my data". The initial use of the Blue Button was in 2010 when the Department of Veterans Affairs deployed the Blue Button initiative as part of its online combined personal health record (PHR) and patient portal, My HealtheVet to allow simple exchange of a patient’s personal health data in a standard, consistent format\(^6\). As of January 2014, the My HealtheVet (MHV) PHR portal has more than 2.6 million registrants (37% of the VA patient population), with more than 1.4 million VA patients having authenticated access which allows for Blue Button access to their health data (25% of the VA patient population). More than 955,000 veterans have used Blue Button and have downloaded over 5.7 million Blue Button files\(^7\).

The Blue Button framework has continued to evolve and in 2012, the Office of the National Coordinator for Health IT (ONC) within the US Department of Health and Human Services took on the responsibility for creating a new framework, in collaboration with the VA, the White House, and a host of other public and private sector leaders. The Blue Button pledge program includes over 500 organizations including healthcare providers, insurance companies, labs, drug stores and most
recently mobile application developers focused on making personal health data available for electronic access and transmission\textsuperscript{6}.

The Blue Button movement is considered a key patient engagement initiative, illustrating this, a May, 2012 study done on over 18,000 My HealtheVet users showed that the most highly endorsed benefit of Blue Button was that it helped patients understand their health history better because all the information was in one place (73\%). Of those patients that shared their Blue Button data with a non-VA provider, 87\% reported that the non-VA provider found the information somewhat or very helpful\textsuperscript{7}. In another study, almost 4 of 5 respondents (79\%) were interested in sharing access to their PHR with someone outside of their health system\textsuperscript{8}.

In this project, we architect an initial design for a cloud based implementation of the Blue Button framework for a commercial laboratory to facilitate patient access to electronic results.

\textbf{Methods}

\textbf{Application Components}

The following application components were designed for this project:

\textbf{Encrypted Data Store Component and API}

The encrypted data store is a private REST interface published via SSL/TLS which requires authentication. Its primary purpose is the storage of encrypted patient data and the retrieval and decryption of data when the appropriate key is presented. A relational Sql based database has been utilized for this project but non-relational "no-sql" databases such as Hadoop or MongoDB are equally acceptable for this type of record storage and retrieval.

\textbf{Client Access Component and API}

The client access API stores the encryption keys for the records contained in the Encrypted Data Store component and re-encrypts these keys utilizing identity-based encryption methods. For the purposes of this initial project, patient last name and date of birth were selected as the key identity attributes for the encryption of these records. The API has been designed to facilitate additional and alternate key
attributes if required. When the appropriate keys and authentication are presented the API retrieves the encrypted data from the Encrypted Data Store via REST and makes it available for presentation or transfer to an authorized provider. The client access API is a REST interface published via TLS.

The client access portal allows for patient registration and retrieval of records when an Encounter ID and the correct identity-based encryption keys are presented. The client access portal also allows a user to select a registered Blue Button provider and authorize Push document transfer of records.

A relational Sql based database has been utilized for the storage of both the encrypted key information and the encrypted patient registration information but non-relational "no-sql" databases such as Hadoop or MongoDB are equally acceptable for this type of record storage and retrieval. To meet the requirements of HIPAA and NIST guidelines, the Client Access Portal component must be hosted on a device (and ideally at a location) separate and distinct from the Encrypted Data Store component.

**Result Publisher Component**

The Result Publisher component is responsible for creation of the patient health record from the Laboratory Information System (LIS) utilizing the HL7 Consolidated Clinical Document Architecture known as the Consolidated CDA (C-CDA). The Consolidated CDA is a XML-based standard that specifies the encoding, structure, and semantics of a clinical document which for Blue Button plus use utilizes the sections and fields specified in Meaningful Use Stage 2. As this implementation is currently limited to the requirements of a commercial laboratory, this record includes the header section (containing patient information and demographics) and the results section which includes laboratory tests. The Result Publisher component is responsible for the encryption and storage of the patient record with the Encrypted Data Store via REST interface and the re-encryption of the resulting key and storage with the Client Access component via REST interface. The Result Publisher also maintains a relationship database which links patient encounters to patient identification systems (i.e Client Medical Record Numbers). These
relationships are published (as encrypted tokenized records) to the Client Access component. Figure 1 shows the core implementation framework.

**Architecture and Methodology**

**Figure 1.** Core implementation framework.

The electronic encounter ID is generated in the laboratory system when the order enters the system. This encounter ID includes a checksum for maintaining integrity and accuracy and is made available to the patient along with information on the web portal at the time of specimen collection. This electronic encounter ID can also be provided to the patient by the customer service center or the referring provider as this information is resulted to their systems.

When results are complete on an encounter id, the Results Publisher component application packages the result in an industry standard C-CDA format. For this
implementation, the Results Publisher operates in the same data center as the laboratory information system and has direct access to result data. The Result publisher encrypts the resulting C-CDA record utilizing AES-256 bit salted encryption and stores the result with the Encounter ID via the REST interface presented by the Encrypted Data Store component. The generated 256 bit encryption key is then encrypted utilizing AES Identity based encryption and stored in the Client Access Component with the Encounter ID via the REST interface. To access the electronic record, a patient creates an account using the portal presented by the Client Access component. As an added security level, in order to activate this account, the patient must validate a telephone number via text message or click on an e-mailed link with a Captcha check (multi-factor authentication). After the account is successfully validated, the patient can enter the Encounter ID (token based authentication) together with their last name and date of birth (identity/attribute based authentication) to view or download the C-CDA document per Blue Button specifications. Because the Client Access component maintains relationship information on multiple encounters by the same patient (within an individual client), this authentication can enable access to multiple encounters. Within the portal, the patient can view registered Blue Button providers and authorize Push (Direct) document transfer of records via Blue Button + protocol to a provider or PHR (Microsoft Healthvault, Dossia, and Indivo Health etc.).

**HIPAA Compliance and Secure Design Protocols**

In architecting this solution, careful consideration has been given to best practices for safeguarding the confidentiality, integrity and availability of protected health information (PHI). This system has been designed to comply with the requirements and guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C, and in accordance with best practices specified by the National Institute of Technology. The application components and storage utilized by the public facing application components and data have been encrypted in accordance with the
HIPAA Security Rule, “Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals”\textsuperscript{14}. Electronic PHI has been encrypted as specified by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. The application components have been purposely isolated as specified in the guidance “to avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt”\textsuperscript{14}. The encryption processes used for data at rest (AES 256/SHA-256) meet or exceed the requirements of the National Institute of Standards and Technology (NIST)\textsuperscript{9}. The encryption processes for data in motion (currently TLS v1.2) are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations and are Federal Information Processing Standards (FIPS) 140-2 validated\textsuperscript{12}. The identity based key system, key encryption standards and use of multi-factor authentication have been chosen based on a review of current best practices and emerging standards in Attribute Based Access Control (ABAC)\textsuperscript{15,16,17}. All data stored and transmitted in this project is handled in such a way as to render PHI unusable, unreadable, or indecipherable so that no breach notification is required following use or disclosure of the stored information under the requirements of HIPAA and HITECH. The Encrypted Data Store component and the Client Access component can be hosted in a cloud environment. The use of cloud computing in healthcare is expanding at a rapid pace, a recent study by the SANS institute showed that 48% of healthcare organizations use cloud computing to process protected patient and financial information\textsuperscript{10}. Cloud computing may become the standard model of operation for health care providers, their affiliates and their clients, such as governmental health and human service agencies\textsuperscript{11}. Of particular note, CMS, issued new standards and conditions in 2011 directing states to “pursue a service-based and cloud-first strategy for system development” as a condition for federal (CMS) funding\textsuperscript{12}.
Results
The resulting application components and programming interfaces accomplish the initial project goals and provide a base to expand the platform to offer support for mobile devices and additional interoperability options. Encryption, isolation and multifactor authentication of data have been used to safeguard the confidentiality, integrity and availability of protected health information (PHI) and allow for the use of standard cloud services to host external facing components.

Discussion
A primary goal of this project was to present a robust solution that would meet HIPAA standards while enabling end users to access their information easily and authorize the transfer of records to other providers in an efficient manner. The resulting design accomplishes this goal and provides an acceptable balance between security, efficiency and timely access to health data. One of the strengths of this solution is the ability to dynamically limit access to the encrypted medical records or change the keys or algorithms used to encrypt the records at any time. As the portal application only grants the user access to encrypted keys, this prevents the loss of PHI in the event of unauthorized access to the encrypted databases. The Result Publisher component, which is secured by a firewall and not accessible via the internet, has the ability to re-encrypt the records or disable access to records. It is important to note that in a commercial laboratory setting, patient results are encounter centric. This solution, through a relationship database maintained by the result publisher component, allows the linking and retrieval of multiple encounters for a patient if all visits are with a single provider. Although it is theoretically possible to allow a patient to link multiple providers, and by extension, multiple encounters within each provider, this functionality has not yet been implemented in this project. It is currently under consideration and review. The ability for a patient to authorize additional updates (i.e. new encounters and results) to be sent automatically as labs are performed (often referred to as Blue Button + push update functionality) is not yet implemented in this project. This is currently under development and it is anticipated that the authorization component
will be performed within the Client Access component but the authorization will be transferred and stored within the Result Publisher. The Result Publisher will manage the transmission of push updates via the Client Access API. This approach is required to limit the PHI stored within the Client Access component for security reasons.

The current project design does not fully implement the BB+ Pull and Oauth2 API required to support mobile applications. This is currently in the planning stages for future development and will be included in the Client Access API.

**Conclusions**

The Blue Button standards and framework provide a solid basis for facilitating electronic access to result data by patients and for meeting the requirements of View, Download, and Transmit (V/D/T) in Meaningful Use Stage 2 (MU-II). The recommended platforms include a variety of protocols for the secure exchange of information, including APIs (Application Programming Interfaces), Secure Attachments, and Web Services. The current Blue Button framework is suitable for allowing patients easy electronic access to laboratory result data for use in personal health record systems (PHR-S) and for transfer to other health providers.

**Conflicts of Interest**

None declared

**Abbreviations**

**AES**: Advanced Encryption Standard  
**AES-256**: Advanced Encryption Standard 256 bits  
**ABAC**: Attribute Based Access Control  
**API**: Application Programming Interface  
**C-CDA**: Consolidated Clinical Document Architecture  
**CDA**: Clinical Document Architecture  
**CMS**: Center for Medicare and Medicaid Services  
**FIPS**: Federal Information Processing Standards  
**HIE**: Health Information Exchange
HIPAA: Health Insurance Portability and Accountability Act
HIT: Health Information Technology
HITECH: Health Information Technology for Economic and Clinical Health Act
HL7: Health Level 7
LIMS: Laboratory Information Management System
MHV: My HealtheVet
MU-II: Meaningful Use II
NIST: National Institute of Standards and Technology
ONC: Office of the National Coordinator for Health IT
PHI: Protected Health Information
PHR: Personal Health Record
PHR-S: Personal Health Record System
REST: Representational state transfer
SANS: System Administration, Networking, and Security Institute
SSL: Secure Sockets Layer
SQL: Structured Query Language
SHA-256: Secure Hash Algorithm 256 bits
TLS: Transport Layer Security
VA: Veterans Administration
V/D/T: View, Download, Transmit
XML: Extensible Markup Language

References

1. Berwick DM, Nolan TW, Whittington J. The triple aim: care, health, and cost. Health Aff (Millwood). 2008;27(3):759-69. PMID: 18474969
2. Schoen C, Osborn R, Huynh PT, et al. Taking the pulse of health care systems: experiences of patients with health problems in six countries. Health Aff 2005;Suppl Web Exclusives:W5-509–525 PMID: 16269444
3. URL:http://www.healthit.gov/patients-families/about-blue-button-movement. Accessed: 2015-05-12. (Archived by WebCite® at http://www.webcitation.org/6YSI2f3pS)
4. Hogan TP, Nazi KM, Luger TM, Amante DJ, Smith BM, Barker A, Shimada SL, Volkman JE, Garvin L, Simon SR, Houston TK, Technology-Assisted Patient Access to Clinical Information: An Evaluation Framework for Blue Button, JMIR Res Protoc 2014;3(1):e18, DOI: 10.2196/resprot.3290, PMID: 24675395

5. Austin R, Hull S, Westra B. Blue button movement: engaging ourselves and patients. Comput Inform Nurs. 2014;32(1):7-9. PMID: 24441169

6. Vogel L. "Blue button" access to medical records. CMAJ. 2010;182(16):E746. PMID: 20921256

7. Turvey C, Klein D, Fix G, et al. Blue Button use by patients to access and share health record information using the Department of Veterans Affairs' online patient portal. J Am Med Inform Assoc. 2014;21(4):657-63. PMID: 24740865

8. Zulman DM, Nazi KM, Turvey CL, Wagner TH, Woods SS, An LC. Patient interest in sharing personal health record information: a web-based survey. Ann Intern Med. 2011;155(12):805-10. PMID: 22184687

9. Scarfone K, Souppaya M, Sexton M. Guide to Storage Encryption Technologies for End User Devices, NIST Special Publication 800-111. Nov 2007

10. Ross R, Viscuso P, Guissanie G, Dempsey K, Riddle M. Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. NIST Special Publication 800-171. June 2015

11. Quirolgico S, Voas J, Karygiannis T, Michael C, Scarfone K. Vetting the Security of Mobile Applications. NIST Special Publication 800-163. Jan 2015

12. Polk T, McKay K, Chokhani S. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, NIST Special Publication 800-52 Revision 1. April 2014

13. Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4. Jan 2015.

14. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act;
Other Modifications to the HIPAA Rules; Final Rule, 78, Fed. Reg. 5566 (1/25/2013) (to be codified at 45 C.F.R. pts. 160 & 164).
URL:http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
Accessed: 2015-05-12. (Archived by WebCite® at http://www.webcitation.org/6YTODcbkf)

15. Hu V, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162. Jan 2014

16. Barker E, Dang Q. Recommendation for Key Management Part 3: Application-Specific Key Management Guidance. NIST Special Publication 800-57 Part 3 Revision 1. Jan 2015

17. Chen L, Recommendation for Key Derivation through Extraction-then-Expansion, NIST Special Publication 800-56C, Nov 2011

18. Filkins B, SANS Inaugural Healthcare Study, 2013
   URL:http://www.sans.org/reading-room/whitepapers/analyst/inaugural-healthcare-survey-34855. Accessed: 2015-05-12. (Archived by WebCite® at http://www.webcitation.org/6YTQ8SH7t)

19. Noblin A, Cortelyou-ward K, Servan RM. Cloud computing and patient engagement: leveraging available technology. J Med Pract Manage. 2014;30(2):89-93. PMID: 25807597

20. Enhanced Funding Requirements: Seven Conditions and Standards, Centers for Medicare & Medicaid Services, April 2011
   URL:http://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Data-and-Systems/Downloads/EFR-Seven-Conditions-and-Standards.pdf. Accessed: 2015-05-12. (Archived by WebCite® at http://www.webcitation.org/6YTRm1Bp7)