Evaluation of Secure Text Messaging Applications Towards the Design of Hc-Messaging

**Matthew A. McDonald**

Towson University

Towson, MD

Mmcdon18@students.towson.edu

***Abstract-***

***Wireless devices, such as smartphones, have great potential in increasing the quality of healthcare. As this domain requires the ability to quickly share information, convenience and speed is of extreme importance. Wireless computing devices provide the potential for increased productivity, the benefit of convenience and accessibility, as well as the ability to lower costs for providers as the majority of the devices needed will already be readily available to employees. However, these benefits are rendered useless in the healthcare domain if the use of these devices do not meet the security and privacy standards of The Health Insurance Portability and Accountability Act (HIPAA) [1]. For this reason, this paper will analyze the security features necessary for a messaging solution to be considered secure and HIPAA compliant. Also, an evaluation of three secure solutions on the market today will be performed, based on these established security features. Finally, the implementation of security features into Hc-Messaging will be developed in order to provide an open-source competitor to the off-the-shelf messaging applications available today****.*

# INTRODUCTION

As we see an increase in hospitals around the nation adopting some form of a BYOD (bring your own devices) policy [2], many providers fear that texting is another way for their organization to be at risk for a HIPAA-related data breach and the associated fines that come with it. However, with a secure solution in place, the valuable communication tool that physicians and patients all have in their pockets can be properly taken advantage of in order to fully utilize its benefits. While a smartphone (and text messaging in particular) offers great potential in the advancement of healthcare, its utilization will not be possible unless it is able to remain HIPAA compliant.

Due to the HIPAA Privacy Rule, and the costly fines that result from non-compliance, it behooves Hospitals and other covered entities to protect patient’s Protected Health Information (PHI) from unauthorized disclosure. Unauthorized disclosure is defined as the exposure of PHI to anybody that does not have a need to see the information, unless authorized to do so by the patient. Any instance of unauthorized disclosure of PHI is considered a data breach [2], and the responsible party is subject to HIPAA-related fines. These facts, combined with the rise of personal devices being used in hospitals, contribute to the need of a secure and HIPAA-compliant solution to view and transmit PHI with the use of a smartphone.

The use of smartphones in the healthcare domain leads to the temptation to use standard SMS services for communication, which would include the transmission of PHI. However, standard SMS messaging is considered an unsecure solution. One reason why SMS messaging is considered an unsecure solution is that messages are sent wirelessly “in the clear” [3], which means they are unencrypted and susceptible to eavesdropping techniques which would be considered a data breach if PHI was intercepted and read by an unauthorized individual. Another reason why regular SMS messaging is considered an unsecure messaging solution is because there is no type of authentication process to ensure that the message is being read by the intended individual. Even if the text message was sent to the correct phone number, it is possible that the phone is currently in another person’s hands, and could be read by an unauthorized individual, which again, would be considered a data breach. Also, with SMS messaging, the data is stored on individual’s personal devices, which can cause problems when trying to recall certain information. For instance, if a doctor wanted to edit a message that was sent, it would be impossible to do so because of the fact that the message sent is being stored locally on the recipient’s device, and not a centralized server. Since we are dealing with mobile devices, the chance of a lost or stolen device is high. Without the ability to remotely recall or wipe a chat history, there is a possibility of PHI being seen by an unauthorized individual in the event that the device is stolen.

Thankfully, there are security features in place today that have the potential to provide secure alternatives to SMS messaging. These features could provide for security if used within a compartmentalized messaging application that would be used strictly for a healthcare domain. For instance, to deal with the wireless transmission of data, we can use end-to-end encryption in order to ensure the confidentiality of the information being transmitted. This would remedy the threat of eavesdropping because the only thing that would be intercepted is cipher text, which would be of no value and would protect the PHI from unauthorized disclosure. Another security feature used to counteract the vulnerabilities of SMS messaging is Application-level authentication. This would provide authentication to ensure that the message being sent is reaching the desired recipient. Application-level authentication could be implemented through the use of a standard username and password credentials, biometric features such as fingerprint/iris scanners, or a combination of both. These type of features would mitigate the threat of the information being seen by an unauthorized individual. In order for a messaging system to be considered “secure”, it would need to implement these features. [4]

A 357-bed Hospital named Waterbury Hospital in Connecticut implemented the use of a secure messaging application with the use of TigerText with their employees [13]. Waterbury Hospital employees integrated TigerText into their workflow in early 2014 in order to provide their physicians with an effective tool to communicate with each other, all while remaining HIPAA-compliant. Waterbury Hospital was able to expand on this communication tool by integrating the messaging application with their existing Electronic Health Record (EHR) system.

Waterbury received excellent results in response to their adoption of TigerText. According to their self-reported metrics, they were able to reduce the average length of patient stays by almost two full days due to the quicker access to information [13]. Due to these lower average length of stays, the hospital was able to save over $2,200 per patient [13].

Despite these positive results, I believe that more work needs to be done in spreading awareness of the benefits of secure messaging systems in the healthcare domain. According to a survey done by Infinite Convergence Solutions in 2016, only approximately 10% of hospitals are currently using some type of HIPAA-compliant messaging system [14]. I hypothesize that the main contributing factor to this low adoption rate is due to the fact that many doctors and health care providers are still using long established workflows that are hard to break out of for tenured professionals. For example, many doctors currently still use pagers and landline phones as their main form of communication in the workplace. Even worse, the survey reported that of the hospitals that are using newer technology as a communication tool, such as smartphones, and tablets, are using unsecure and non-compliant messaging solutions such as Hangouts, WhatsApp, and Facebook Messenger [14].

# BACKGROUND / RELATED WORK

There are currently solutions available on the market today that claim to offer a secure messaging service that is HIPAA-compliant, and therefore could be used confidently in a healthcare domain. We will first formally define all the necessary requirements of a HIPAA-compliant messaging service, and then we will critique three of the available solutions on the market today, based on these established security features.

We have already touched on the necessary security features of a HIPAA-compliant system. To recap, these features are end-to-end encryption [5] to provide confidentiality of the data being transmitted. The second feature we have covered is application-level authentication [5], which is necessary to ensure that the message is being read by its intended recipient. Finally, we have covered the fact that we want all data to be stored in a secure cloud environment, with no PHI being stored locally on personal devices. This will provide for features such as the editing/recalling of messages, as well as remote wiping and lockout features if a personal device is reported missing or stolen [6]. All of these features are in addition to the messaging occurring in its own compartmentalized application specific to the healthcare domain, compared to being integrated with personal messages, which could lead to the accidental data leakage of PHI [6].

With these established security features, we will survey three of the current self-proclaimed HIPAA-compliant messaging services on the market today to see if they can be considered a secure solution. The four applications we will review are TigerText, DrFirst, AthenaText, and DocHalo.

## *A. TigerText*

We will first evaluate TigerText based off its use of encryption to provide confidentiality. TigerText transmits messages using Advanced Encryption Standard (AES) 256-bit/SSL end-to-end encryption [7]. This implementation satisfies the required security feature needed to ensure confidentiality of the data being transmitted. The second security feature that we will evaluate TigerText on is the use of application-level authentication. TigerText does indeed provide this feature via the use of usernames and passwords that are provided access by an admin, and authentication must occur in order to be able to send messages [7]. After initial sign-up, invitations can be sent to others in the organization for use of the application. Finally, the last security feature that we will critique TigerText off of will be the use of a secure cloud to store the message data. This is also provided by TigerText. The data centers that TigerText stores its information on are stored at-rest with AES 256-bit encryption [7], and they are also backed by a SAS 70 Type II certification for additional security [7]. Not only does TigerText provide the implementation of the three required security features, they also offer a $1 million guarantee that their platform will remain private and secure [7]. According to [www.totalhippa.com](http://www.totalhippa.com), they are the only secure messaging platform to offer this type of guarantee. One drawback of the TigerText application is the cost. While exact pricing information is unavailable, TigerText requires you to reach out to them for a quote, indicating that their solution is not free.

## *B. DrFirst*

The second messaging application we will critique is called DrFirst [8]. To ensure confidentiality of the messages being transmitted, DrFirst uses HTTPS encryption to protect the messages and patient data [8]. This satisfies the requirement of encrypting the messages being sent. The second security feature needed for a messaging application to be considered HIPAA-compliant is the use of application-level authentication. DrFirst also satisfies this requirement by implementing a username/password based login system which is controlled by an assigned administrator [8]. Finally, the last security feature necessary for an application to be considered HIPAA-compliant is the use of a secure cloud server to store the data, contrary to regular SMS messaging which will store the data on the personal devices. This too is satisfied by DrFirst as they use their application is operated and maintained behind DrFirst’s secure firewalls, with access only via SSL web services and maintenance VPNs [8]. No data is stored on the personal mobile devices, so any information transmitted via DrFirst remains confidential. Again, DrFirst does not offer public pricing information, an inquiry must be made to them directly in order to determine the cost of using this application within a specific domain.

## *C. AthenaText*

Next, we will critique the messaging application AthenaText based off of required security features to determine if it can be considered a secure solution. AthenaText implements the use of encryption when transmitting communications through AES256 on iPhone devices and AES128 on Android [9]. This satisfies the confidentiality requirement of messages being transmitted. AthenaText also incorporates the required application-level authentication. They do this by requiring users to enter their PIN once the app enters the foreground, at a predetermined frequency which can be adjusted in the settings [9]. The PIN can either be required immediately, after one minute of inactivity, or after five minutes of inactivity [9].

AthenaText handles the third requirement of storing the message data on a secure server in a unique way. Messages sent (encrypted) from a mobile application are routed to AnethaNet [9], which is AthenaText’s secure cloud server. However, the message is only stored there until the intended recipient’s device connects to the network, and the AthenaText application checks for new messages. Then, the message is sent (still encrypted) to the personal device, where it is stored until deleted [9]. Although this implementation provides for end-to-end encryption of the messages, this implementation cannot be considered a HIPAA-compliant solution. The reason for this is because once the message reaches a user’s personal device, there is no way recall or edit that message if the device fails to connect to the network in order to retrieve that request. Ideally, we do not want any data being stored on the personal devices, so AthenaText would not satisfy the requirements of our established security features.

## *D. Doc Halo*

Doc Halo satisfies the need for encryption by encrypting data at all levels. This includes the encryption of data in the database, with the use of 256-bit AES encryption, and the encryption of data in transit, with the use of Secure Sockets Layer (SSL) 2048 bit encryption. This use of encryption competently satisfies the confidentiality requirement. Another requirement of a secure, HIPAA-compliant messaging system is application-level authentication. Doc Halo provides this with the use of username and password authentication method. There is an opportunity for improvement here with the use of biometric authentication features available on mobile devices.

The third security requirement being evaluated, storing message data on a secure cloud server, is also handled correctly with Doc Halo. Again, the data is securly stored on the cloud server via the use of 256-bit AES encryption while the data is at rest. The benefits of storing the data on the secure cloud allows Doc Halo to implement their 30-day maximum lifespan of all messages. This also provides for the ability to remotely wipe the mobile app in the case of a lost or stolen device.

## *E. Comparison*

A common theme found throughout these messaging services is that they all implement a core set of security features in order to be deemed HIPAA-compliant. These security features include: Application-level authentication, the storage of data of a secure cloud, encryption of the data in transit and at rest, full auditing capabilities, and remote lockout/wipe capabilities. All of these security features contribute to HIPAA-compliance in a unique way.

Application-level authentication is necessary for a messaging service to be considered HIPAA-compliant. Authentication features allow for the ability to ensure that the messages being sent are reaching the desired recipient. As a reference, regular SMS messaging is not secure because there is no way to ensure that the message being sent will be seen by the authorized recipient.

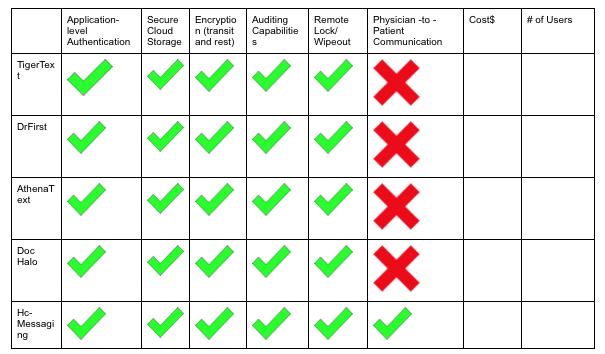
Application-level authentication alleviates this concern because, even if the mobile device is in someone else’s hands, the messaging application (and therefore the sensitive data in the messages) cannot be accessed unless proper authentication is validated. Examples of the implementation of authentication include examples such as typical username and password combinations, or more advanced techniques such as biometric authentication in the form of fingerprint and iris scanning, and/or facial recognition.

Next, having the message data being stored on a secure, private server instead of locally on the user’s mobile devices is another feature that contributes to the security of the messaging services. Due to the nature of mobile devices, they are much more prone to being lost or stolen. This leads to the increased possibility of these devices falling into the wrong hands. With the message data being stored on a secure private server (cloud), instead of on the device itself, the threat of a data breach is severely reduced. Having the messages being stored on a cloud server allows for features such as timed-deletion of messages, read receipts, and universal syncing of conversation history throughout multiple devices.

Encryption is a core feature of data security and the heart of secure messaging services. Regular SMS messaging is insecure because messages are sent “in the clear” and can easily be intercepted and viewed by unauthorized individuals. This is obviously a huge concern when dealing with sensitive data such as PHI. In addition to encrypting the communications in transit, ensuring that the device itself is encrypted would allow for pictures and other sensitive information that has yet to be sent is also encrypted. Again, due to the nature of mobile devices, the likelihood of a lost or stolen device is increased exponentially. For this reason, we need the device to be encrypted in order to prevent the threat of data being stolen from a lost device.

Also, in order for a messaging system to be considered HIPAA-compliant, they must be able to be fully audited by security professionals to confirm that no HIPAA-related data breaches have occurred. Regular SMS messaging falls short in this area due to the fact that chat history is unreliable and shaky at best. This stems from the fact that the messages are stored on the personal devices themselves, and therefore can be deleted from one device and not the other. This leads to inconsistent chat history and limited ways to verify conversations.

Finally, as previously mentioned, mobile devices are naturally at a much higher risk of being lost or stolen. If these devices do end up in the wrong hands, the ability to lock the phone and delete any conversation history remotely will greatly decrease the risk of a HIPAA-related data breach. With all conversations occurring inside the compartmentalized application, combined with the authentication feature, the ability to lockout a user from the application is made possible. In addition, due to the fact that the message data is being stored on a private, secure, and remote (cloud) server, the conversation history can easily be wiped to provide additional insurance against an unauthorized.



*Figure 1 : Comparison Chart*

## *F. Hc-Messaging (Proposed Solution)*

We have seen that two of the three messaging applications we critiqued provide the necessary security features in order to be considered a secure HIPAA-compliant messaging service. These two applications, TigerText and DrFirst, had a shared drawback which is pricing. To provide a solution to this drawback, I am proposing to replicate a messaging application with one of the security features through the use of open-source technologies, in order to provide a fully open-source solution. An open source solution would allow for the opportunity to leverage the expertise of the community, while offering a free alternative to the off-the-shelf options.

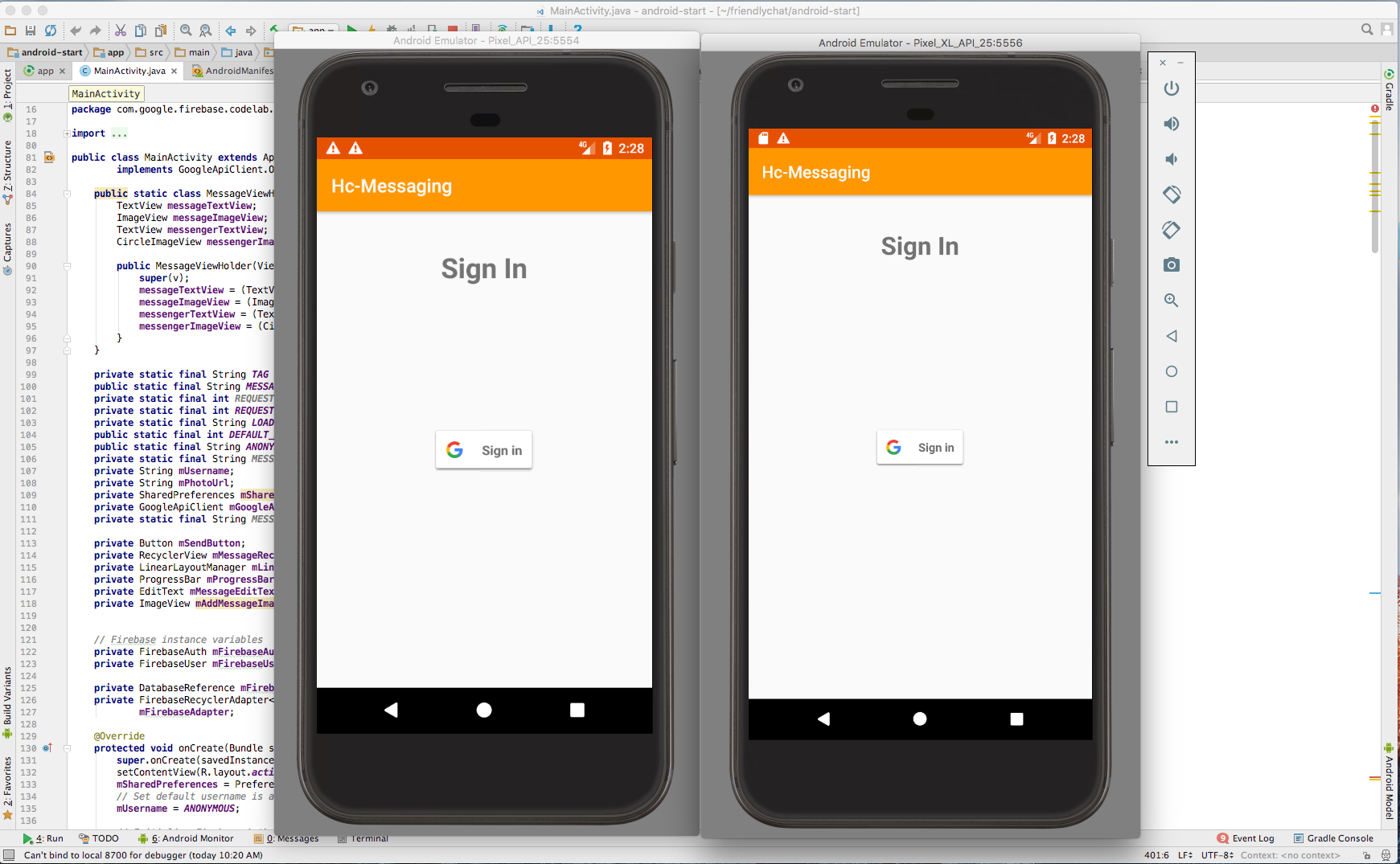


Figure 2: Hc-Messaging Log In Screen

To implement this solution, I used Google’s Firebase, which is a mobile and web application development platform [10]. Firebase offers a cloud messaging solution for Android, iOS, and web applications which can be used at no cost [10]. The use of Firebase would solve the need for two of the security features we have defined. Firebase would allow for the data to be stored on a secure cloud, and it would also provide application-level authentication in the form of Google credentials.

Firebase provides the feature of having data stored in a secure cloud environment. Firebase is hosted on Secure Sockets Layer (SSL), which is a security technology which creates an encrypted link between the host and a client [10]. By default, Google Cloud Platform (which Firebase is built on top of) encrypts data that is being stored at rest. This will satisfy the established requirement of storing the data on a secure cloud [10].

To provide application-level security in my application, I implemented Firebase’s Authentication SDK, which provides a method to allow users to sign in with their Google accounts [11]. Through this, I was also able to incorporate two-factor authentication via the Google application to provide an extra layer of security. This authentication feature would ensure that only valid users were able to log into the application, and hence send and receive messages which may contain PHI.

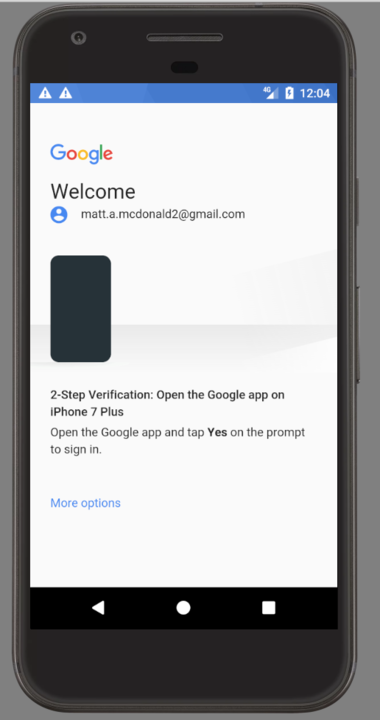
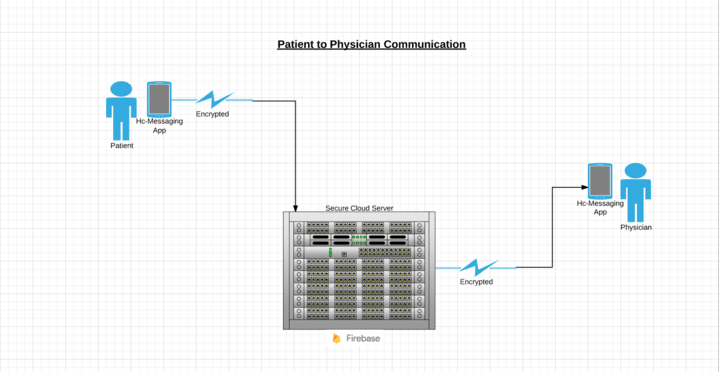
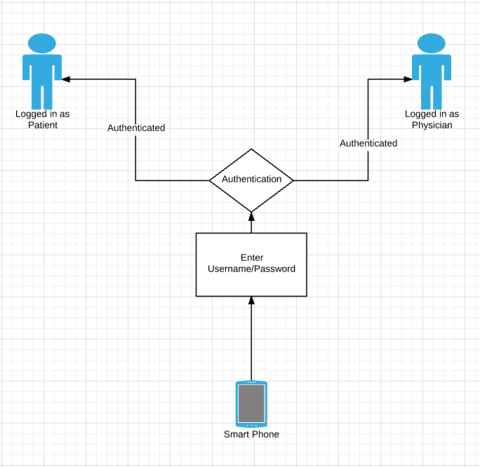


Figure 2: Two-factor authentication

## *G. Design*



*Figure 3: Data Flow Diagram*



*Figure 4: Authentication Flow Diagram*

# ANALYSIS & PERSONAL CRITIQUES

In conclusion, I believe there is great potential for the use of smartphones and other personal devices in the healthcare domain as long as it is done in a secure and HIPAA-compliant way. The technology and security features necessary to provide a secure messaging solution are available and can be implemented to leverage the power of smartphones and other mobile devices. As the use of these mobile devices continues to increase, so too does the need to provide data security and privacy, especially when dealing with the sensitive information in a health care domain. We must continue evolve in order to leverage the technological power of these devices, while maintaining the privacy that we all deserve.

# REFERENCES

1. "Encryption At Rest | Google Cloud Platform". Google Cloud Platform. N.p., 2017. Web. 20 May 2017.
2. "Health Insurance Portability And Accountability Act". En.wikipedia.org. N.p., 2017. Web. 20 May 2017.
3. "HIPAA Compliant Text Messaging Application Review - Total HIPAA Compliance". Total HIPAA Compliance. N.p., 2017. Web. 20 May 2017.
4. "HIPAA-Compliant Messaging 101". Imprivata. N.p., 2017. Web. 20 May 2017.
5. "How Secure Is Your Firebase? – Google Cloud Platform — Community – Medium". Medium. N.p., 2017. Web. 20 May 2017.
6. "Is Texting In Violation Of HIPAA?". HIPAA Journal. N.p., 2017. Web. 20 May 2017.
7. "Secure Text Messaging For Healthcare That Is HIPAA Compliant". DrFirst. N.p., 2017. Web. 20 May 2017.
8. "Secure Texting Product Features | Tigertext". Tigertext.com. N.p., 2017. Web. 20 May 2017.
9. "The Necessity Of Creating A Hospital BYOD Policy: Lessons From Penn Medicine | Healthcare Informatics Magazine | Health IT | Information Technology". Healthcare-informatics.com. N.p., 2017. Web. 20 May 2017.
10. Toth, Cheryl. "Five Ways To Ensure Secure Text Messaging In Your Medical Practice: Page 2 Of 2 | Physicians Practice". Physicianspractice.com. N.p., 2017. Web. 20 May 2017.
11. "Waterbury Hospital Case Study". TigerText. N.p., 2017. Web. 20 May 2017.
12. “90% of Healthcare Institutions Employee Non HIPAA-Compliant Messaging Apps”. Healthitoutcomes.com N.p., 2017. Web. 20 May 2017
13. "Why Are 90% Of Hospitals Not Using Secure Messaging? - TELMEDIQ". TELMEDIQ. N.p., 2017. Web. 20 May 2017.
14. “Why Most HIPAA Compliant Texting Apps Fail – TELMEDIQ” TELMEDIQ. N.p., 2017 Web.