Secure System Proposal

For

NOLA Life

Joshua Haws | Cathy Kennelly | Drake Loud | Jason Smith

1 Cover Letter

February 10, 2016

Office of the CEO

NOLA Life
213 NOLA Life Lane
Nashville, TN 37067
2016 SECURE SYSTEM ANALYSIS

As requested, this is the report regarding the recent concerns raised about NOLA Life's current security policy. The report, policy, and accompanying video presentation compiled by our team of Information Systems Specialists detail the security needed for this new system and outline the technology recommended to meet the system specifications desired.

The team responsible for the contents of this report consists of the following members: (a) Joshua Haws, who led the team in research and headed off the project; (b) Cathy Kennelly, who specializes in user experience and training; (c) Drake Loud, who specializes in software security; and (d) Jason Smith, who specializes in security within specific technologies.

The report details how the proposed new system can provide utmost security to NOLA Life's clients, as well as saving both the client and agents time and money. In addition, the report will suggest the specific technology as well as the key policies needed to ensure the level of security desired by NOLA Life. Please review the following report for more information.

Sincerely,

Office of Information Technology

2 Executive Summary

2.1 Purpose

Changes in NOLA Life's basic processes have triggered not only an evaluation of the new hardware and software to implement, but also the security policies that should be in place. This report will provide a brief analysis of those security policies. This plan is specifically tailored to NOLA Life's new system. This plan will also help resolve any security concerns in regards to the hardware, software, telecommunication and protocols, and user processes of NOLA Life.

2.2 Conclusions

After careful analysis of NOLA Life's current processes, the team was successful in finding problem areas that can be improved through the use of new tablets. These tablets have been selected according to the strictest security concerns. The software and telecommunication protocols have also been carefully selected with security in mind. As NOLA Life plans to have its agents do much of the medical testing and data gathering in the field with the proposed tablets, HIPAA compliance and customer experience have also played large roles in decision making throughout the process.

2.3 Recommendations

The following are the recommendations of the different parts of the project that are being proposed:

2.3.1 Hardware

Fourth Generation Apple iPad Mini's running the latest versions of iOS, 9.2.1 have been chosen for the major hardware for the project.

2.3.2 Software

We recommend purchasing a software package to be used in parallel with the iPad. The specification of the software package can be found in this proposal.

2.3.3 Telecommunications and Protocols

AES encryption and the use of a VPN connection will be used. When the VPN connection is established, SSH file transfer will be used to transmit the information to NOLA Life's servers.

2.3.4 User Process/Training

Training on the correct use of the system will occur in the first two weeks for every new hire. In addition, every two fiscal quarters, employees will be required to take a refresher training course to maintain proper use of the system.

2.4 Introduction

NOLA Life is a mutual insurance company with a rich history of over 125 years. NOLA specializes in whole life and term insurance; they also offer annuities as well. NOLA's network of agents are across the United States and act on behalf of the company to serve individual clients' needs. These agents work with prospective clients and also help advise and evaluate new clients. The procedure to sell and service claims and life insurance to a client is costly and paper intensive.

2.5 Current Process

NOLA Life has been undergoing several procedural changes in order to enhance their business processes. The main focus of the changes in their processes is to provide agents with a technical solution for collecting and processing client information. The use of technology will allow insurance agents to forego their previous method of collecting client information on paper documents, and mailing them to the NOLA Life offices, with the possibility of scheduling a medical technician visit to collect further information.

Through the use of this technology, agents will be informed of new clients, collect information with fewer errors, confirm client's identity, collect medical information, as well as securing customer payment. NOLA Life feels this solution is going to help them going forward because it will allow them to place a priority on improving the customer experience, while cutting down the time and costs associated with their process.

Most importantly this new process will also ensure a high level of security. NOLA Life has yet to determine the specifics of their new process, and have come to our team to propose the potential specifications and needs to ensure the success of this new project.

With these new system specifications in mind, our team proposes the following solutions to help them achieve their business goals in the implementation of this new process. We will address the hardware, software capabilities, telecommunication and protocols, user processes and security training recommendations to achieve the highest level of performance with the new system in place for NOLA Life. In addition, we will outline specific policies to help maintain the high level of security that NOLA Life desires to best serve their clients.

3 Proposal

3.1 Hardware

We have selected a fourth generation Apple iPad mini running the latest version of IOS, which is currently 9.2.1. This device has all of the features that seem essential for Agents to securely use your new system and process, and is also one of the most mature of devices on the market, which brings a lot of reliability and management resources. We will explain how it helps meet the requirements of this project, and some of the reasons that we selected this device over other types of devices.

The iPad mini can connect to Wi-Fi or use a cellular data connection that allows the device to connect in many more areas where secure Wi-Fi may not be available. We think that these having a cellular data connection will allow the data to be much more accessible to agents in the field, and allow the data to be transmitted back to the servers at NOLA Life's headquarters much sooner in most cases. A cellular data connection is often seen as more secure because it does not have shared visibility of other devices in the same way that Wi-Fi is so there is less risk of others intercepting the data during transmission.

The device comes with encrypted device storage to help protect data that must be temporarily stored until it can be transmitted. There are very few other tablets on the market that come with encryption enabled by default, and many other devices suffer a significant performance hit when the encryption is enabled.

The device comes with biometric authentication to allow the device, installed applications, and data stored on the device to be secured from unauthorized users. Biometric authentication is available on very few Android devices, and many have a severe vulnerability that would allow the fingerprint data to be stolen.

Since IOS version 7 was released in late 2013 apps have been able to be programmed to use VPN to allow safe transmission of data, without any extra configuration or hassle for the user. The same feature was not available in the Android operating system until version 5 (Lollipop) was released the following year, and may be less reliable. There are a few different ways to protect data if the iPad has been jailbroken. The application can have data protection enabled which performs a software level encryption on data stored in the app. These encryption methods help to make sure that the data is protected within the environment of the operating system, but if the device is jailbroken these methods will fail, because the operating system is no longer able to do its job protecting the data.

We would recommend an Enterprise Mobile Device Management system like IBM MaaS 360, Jamf Casper Suite, or SAP Afaria, which are able to enforce certain policies, and grant provisional access to an application only if all of the requirements are met. A few of the common conditions that can be enforced are requiring a more complex password to open an app, restricting whether data can be copied or pasted to or from an app, and denying access to an app if the device has been jailbroken. Enforcing conditions like these can help ensure remote wipe if the device is lost, help prevent data leakage, and help with HIPAA, and PCI compliance.

3.2 Software Capabilities

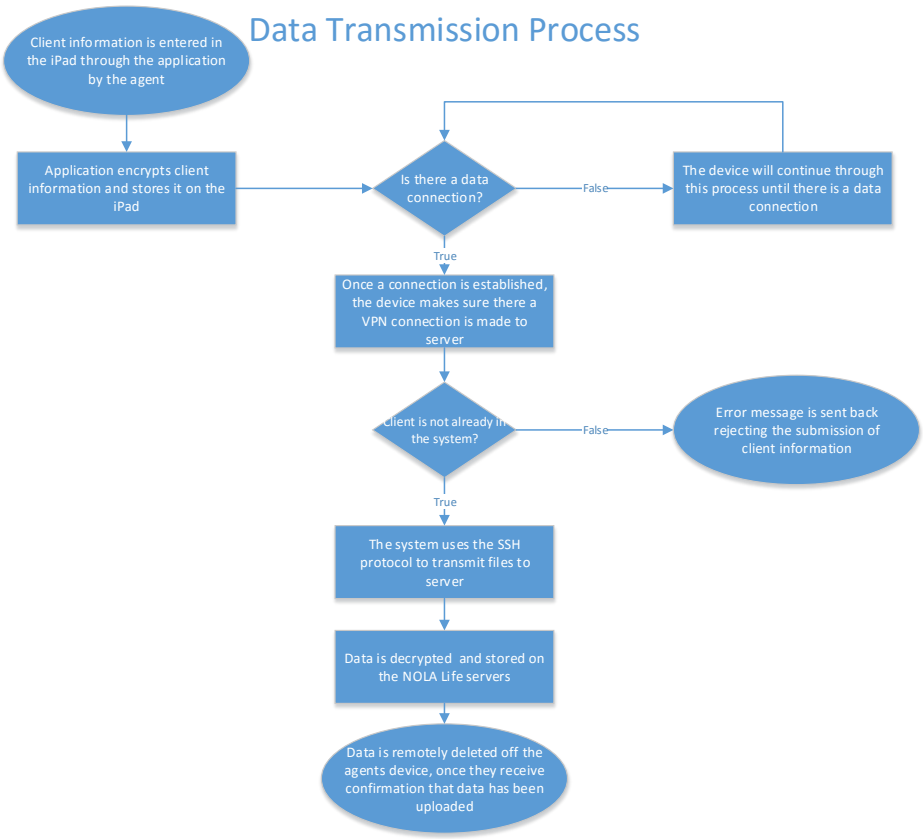
Our proposed hardware should be complemented with the following recommendations in software. As NOLA Life does not specialize in software, a software package is recommended to be purchased with some of the following capabilities and features in mind:

- As the software will be run via iPad, notifications should be silenced so that sensitive information is not accessible from the lock screen, especially to keep in line with HIPAA compliance.
- A secure connection should be required at any time when transmitting sensitive data. If a secure connection cannot be established, data should be encrypted and stored locally on the device.
    - The secure connection should be through the company's enterprise VPN using the VPN connectivity of the device.
- Accessing the device and application should require dual-factor authentication. Biometric access via thumb print should also be required again before accessing highly sensitive information.
- The application should have a time-out after a short period of time.
- The tablet / device should have the option to remote reset the iPad. This will delete all records and information from the device. Members of NOLA Life’s Tech Support Team should have access to this feature.

- Automatic updates should be implemented so that the software is in minimal danger from zero day attacks.
- A Customer Relationship management tool that allows agents to be informed about new customers that they will be serving.
- Inputs need to be validated with different basic checks before submission to ensure that data is clean before arriving at the server.
    - range checks
    - validity checks
    - closed loop authentication
- Payment will be via credit card reader. In the event that payment can not be issued, the credit card information must be encrypted and stored until a secure connection can be made.
- Basic access controls should also be implemented so that only agents with authorization of individual customer's records have access.
- The software should also implement application wrapping to ensure that management can administrate the software as needed.
    - Software application wrapping will also allow the agent to use the iPad for personal use because of the management layer over the software.

3.3 Telecommunications and Protocols

The telecommunications protocols, and the data transmission policies are essential in sending and accessing customer data in a secure manner. We've provided a diagram illustrating the procedure of how data will be transferred from the agents in the field to the NOLA Life servers.



As the diagram illustrates, customer data is collected by the agent through the application. The application will then encrypt the data using AES encryption, and store it locally on the agent's device. The application then will check to see if our device has a data connection through Wi-Fi or cellular data connection. If we have a data connection, we establish a VPN to the NOLA Life network, but if we don't have a data connection the data will continue to be temporarily stored on the device until a connection to the internet is made.

When it is confirmed that we have a secure connection to the NOLA Life servers through a VPN connection, the customer data is then transmitted to the servers though use of the SSH networking protocol. When the data arrives to the NOLA Life servers receive the data it is then decrypted and stored. After it is confirmed that our data is on the servers, the data that was locally stored on the agent's device will be deleted.

Within our process we plan to use AES encryption when encrypting and decrypting data, because it will add a higher level of security. We decided to use a VPN because it's built upon the IPSEC protocol that allows us to uses cryptographic security services to protect communications over Internet Protocol networks. A VPN provides us with security and allows us to create a tunnel that will allow us to connect to part of NOLA Life's private network in public locations. SSH can be used within the VPN, and it will be the protocol by which we transmit the data because it is a secure connection for sending data across a

network. These protocols and procedures will provide the means NOLA Life needs in order to maintain a high level of security of their data, and reduce the potential losses that can happen during data transmission.

3.4 User Process/Training

For our user process policies, we recommend a structure that gives the user (agents handling the devices) a very clear understanding of how the technology should be used. These devices will be used to access client information and due to the sensitivity of this information, it should only be accessed when in the proper situation. For example, when an agent is visiting a client, it is acceptable to pull their private information from the application and download it locally on the device.

After the meeting, the agent has the ability to clear the device of all sensitive information. Regardless, the system will automatically wipe the device of stored information after eight hours of use, after pulling sensitive information from the database. There will be a warning one hour prior to the wipe, to let the agent upload any changes made to records. Our software and hardware recommendations allow the agents to use the tablet for personal uses as well.

Training is an important part of the new system, and we recommend addressing it by having clear guidelines. The first, is to have training take place upon the first week of every new hire, and then repeated every two fiscal quarters. In this training, we recommend reviewing in detail the user process policies, as well as basic technology security.

For the application agents use to pull client information, this would include maintaining secure passwords with least 8 alphanumeric characters, both upper and lower case letters, and at least one special character. Users are required to use unique passwords that have not been used in the past. In order to gain access to the device, we recommend requiring a passcode to keep the device locked. Each employee will be required to change their password every six months, and they may not share their password with others.

Additional basic technology training will include practices such as only using approved software, locking down their devices when not in use, and never opening unsolicited emails and attachments. The training session will also demonstrate the company's top-down security culture, which starts with the management strictly adhering to security policies, and expecting and encouraging the same from their employees.

4 Recommended Policies

4.1 Business Continuity/Disaster Recovery Plan

Data only has value as long as it is accessible when and where it is needed to make business decisions, and it must be protected to ensure that only those who need access are able to view the data.

In order to help make sure that the agents are able to get help if their device is lost, damaged, or fails, we would recommend having a dedicated team of technical support representatives who are able to assist with common issues.

There are some issues that agents may face that would be difficult for a technical support representative to solve, especially considering the nationwide distribution of agents, and so we would recommend purchasing Applecare for Enterprise because it has many valuable services. Applecare for Enterprise is a partnership service offered by Apple, and IBM who has certified technicians who can make next-day support visits on-site for agents most anywhere in the world. It also extends Apple's traditional warranty to allow you to replace up to 10% of your devices each year for any reason, and you they offer an additional year of protection beyond the two-years that is available with the standard Applecare service. They can also help with the deployment, and management of the devices in your organization.

In order to protect the data entered on the device we recommend that the application be set to be wiped after it has been successfully transmitted which can help minimize the risk of it being accessed if the device is lost or stolen.

There are still some areas of the nation where a data connection is not available to send the data, so if data is not able to be transmitted it will be stored locally in encrypted storage. If an agent has to have access to customer information in one of these areas they should be able to pull that data from the servers to the device, but the application should erase that data after 8 hours.

4.2 Prevent Duplication/Data Loss

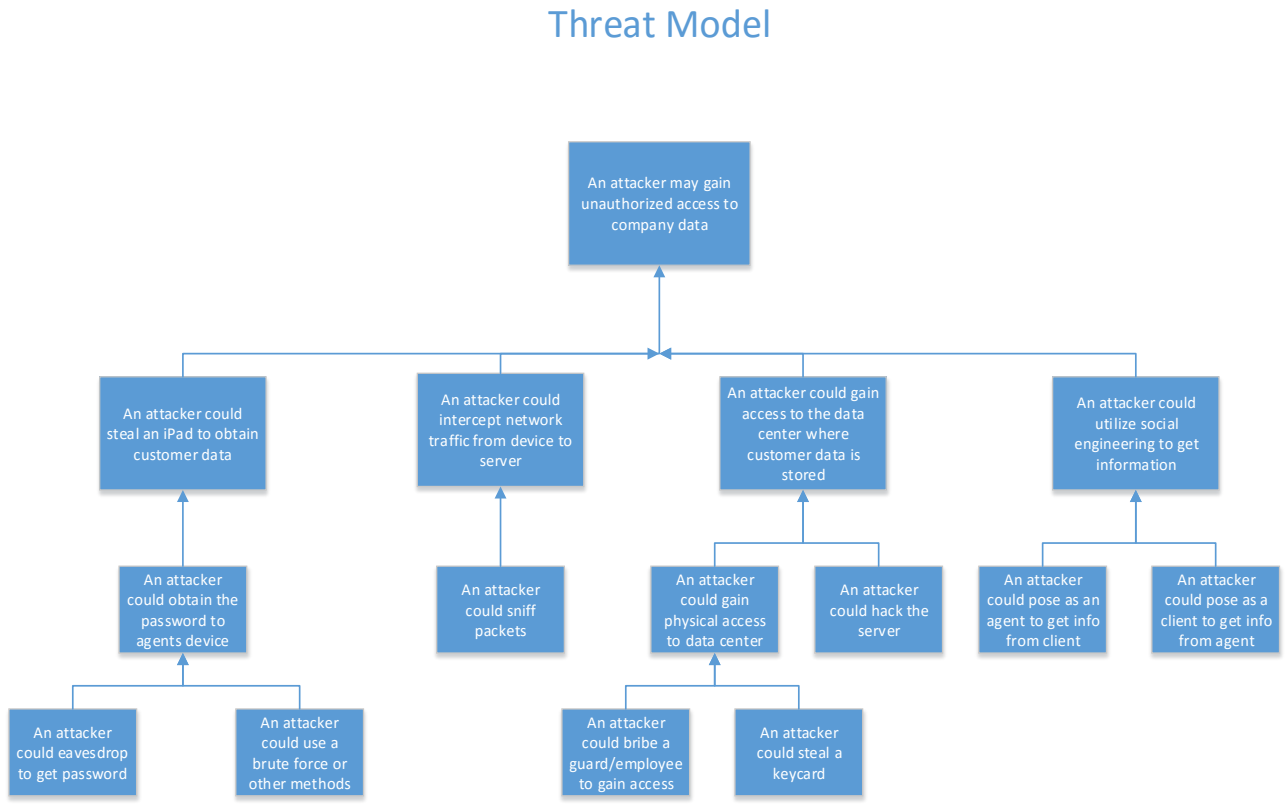
A couple of the greatest benefits of moving to an electronic system is a reduction in the duplicate copies of data that are required for multiple people to have access to the same information, and additional options for preventing data loss. In a digital system there is still potential for duplicate data to be entered, but there are a few things that can help minimize that risk. We suggest using the client's Social Security number as a unique identifier in our database tables to avoid duplication of a client record.

In a world of portable devices, a potential risk of data loss could be due to an exhausted battery causing a power failure during a form submission or transmission. To help prevent

this we would recommend that agents be provided with multiple device chargers, and a portable battery to allow the devices to be charged during the day if the device batteries are found to be near exhaustion.

5 Threat Model

In order to provide the highest level of security, all levels of access and theft must be acknowledged and addressed. One way to visually determine the different vulnerabilities in a system is through a threat model, which we provide below. This model pinpoints different threats, and how those attacks could be accomplished. By establishing all the various ways an attacker could breach the system, we can place security in those positions to protect against threats.



6 Justification

6.1 Cost/Benefit Analysis

Because implementing the new policy has associated costs, an analysis of the costs and benefits associated with implementing the new policy is necessary. As detailed in the following discussion of costs and benefits, the cost of implementation is only a fraction of the monetary value created by the proposed policy. The new policy will add value by mitigating the risk of exposure caused by data loss and increased security, while the reducing the costs of medical technicians, and general business overhead.

The bulk of the costs involved with implementing this system are one-time expenses, including hardware and software required to facilitate the added security measures for the system. The list of expenses was estimated using average costs for these items produced by the Department of Education Information Technology Security, and the cost for the new support team was estimated using the average salary of IT support professionals.

Costs			
iPads	200	$ 399.00	$ 79,800.00
Medical Device/Card Reader	200	$ 300.00	$ 60,000.00
Tablet Antivirus	200	$ 5.95	$ 1,200.00
Enterprise Apple Care			$ 21,800.00
Compliance Audit			$ 40,000.00
Training			$ 870.00
Tech Support			$ 55,000.00
		Total Costs/Year	**$ 258,670.00**

Benefits			
Reduced Medical staff	4	$ 50,000.00	$ 200,000.00
Reduced Overhead			$ 86,297.00
Reduction in Expected Loss			$ 1,365,000.00
		Total Benefits/Year	**$ 1,651,297.00**

The initial expenses total to about $258, 670. However, in just the first year, the new security implementations are expected to reduce the impact of expected loss from $1.5M to only $140,000, a difference of $1,365,000. These figures were calculated using the conservative estimation of $3.5M for the average industry loss due to security incidents multiplied by the 43% chance of an incident compared to the 4% chance of something happening with the new security measures (Ponemon 2014). The cost of implementation and the expected loss with the new systems yield a return on investment of $1,651,297 in the first year alone.

A cost-benefit analysis reveals that even with an initial outlay of $258,670, the proposed system still provides a 638% return on investment within the first year which translates to a $1,651,297benefit. Additionally, as NOLA Life gains a reputation for being secure and safe,

customers will feel more confident trusting their investments with NOLA Life. In other words, implementing the provisions outlined by the proposal will not only save NOLA Life's money, it will also aid in the generation of clientele and revenue by an improved through an improved customer experience, as well as assuring the clientele that their data is secure.