Whitepaper

Mobile Messaging in the Healthcare Sector

Published: 00 Month 2018

www.adeya.ch

Download printable version here: https://adeya.ch/

over
$7.8bn
Smartphone subscriptions globally

over
2.48bn
Estimated messaging app users by 2021

25%
Estimated increase of mobile technology market by 2023.

Part One:

The Mobile Messaging Security Landscape

In 2016, smartphones made history - more people used a smartphone than a desktop to access the Internet[1].

This tipping point is reflected not only in the consumer space, but also in business, with industries like healthcare embracing mobile technology. In healthcare, this is translated into a 25% growth in the market for mHealth to 2023 [2]. There are now 7.8 billion smartphone subscriptions globally - that is a smartphone for almost every human on the planet [3]. As we move further into the 21st century, modes of working are becoming more fluid and mobile communications are essential to enabling this fluidity. This is also being reflected in the healthcare sector where over 80% of physicians use a smartphone at work [4].

The freedom offered by mobile communications is one of the driving forces behind a more innovative way of working. Mobile communications enable a business to reach outside of geographical boundaries to find the best person for the job. It gives the organization and its workforce the tools to communicate within teams, with patients, and with other business associates in a seamless and engaging manner. The mobile workplace is the workplace that communicates.

This shift in communication is evident in the rise of the mobile messaging app. With remote teams and teams in the field, having a messaging app can be crucial to fast responses in time sensitive situations. Mobile messaging has seen a surge in use among consumers too, with an expected 2.48 billion messaging app users by 2021 [5]. This is being reflected in the business and healthcare world as people use smartphones to research healthcare matters - the next step being messaging apps used by healthcare professionals to communicate potentially sensitive and confidential information. A study by Radicati [6] shows that mobile messaging is expected to steadily increase until 2022; with an open rate for a mobile message of 98% compared to 22% for an email, it is a compelling use case.

But other less positive forces are coming into play: as we change our business models and embrace new technologies, we also open up opportunities for malicious forces.

MOBILE MESSAGING MINDFULNESS

Benefits of Mobile Messaging

Mobile messaging within an organization has a number of positive forces that are too compelling to ignore.

This is in line with modern workforce expectations of a more open workplace, as well as, for example, using new technologies for better patient outcomes. Among the benefits of mobile messaging are:

IMPROVED PRODUCTIVITY:
In a report by Aruba Networks(6) 60% of employees said a mobile-first business made them more productive.

EMPLOYEE SATISFACTION:
The digital workplace is seen as an attractive one.

ACCOMMODATING WORKERS IN THE FIELD:
Mobile messaging allows a business to look further afield in recruitment and build effective remote teams.

REDUCED RESPONSE TIME AND SEAMLESS WORKFLOW:
The instant nature of mobile messaging keeps work flowing.

IN HEALTHCARE EVEN MORE BENEFITS ARE OBSERVED:

IMPROVE CLINICAL CARE QUALITY:

Clinical quality is vital for better patient outcomes, as well as better relationships between patients and caregivers. A survey looking at how mHealth improves care quality, found that when using an mHealth approach, data duplication decreased by up to 92% and collaboration improved. The survey conclusion was"...the adoption of appropriate mobile solutions had the potential to significantly improve productivity, efficiency and safety, and could allow services to continue to provide high-quality care with good outcomes. [8]

IMPROVE RE-ADMISSION RATES.

Re-admission is a serious issue for healthcare which mHealth can help improve. Various studies, including one by Penn Medicine's Penn Care at Home [9] have shown that with seamless and swifter communications between patient and healthcare services re-admission rates can be reduced.

COST SAVINGS AND SPEED:

A study into remote monitoring of patients using mHealth found cost reductions of $8000 per patient per year [10]. Another survey by RedHat, found that 30% of nurse-call systems will be replaced by real-time communications and collaboration by 2019 [11].

THE MOBILE MESSAGING SECURITY LANDSCAPE

AS ORGANIZATIONS INCREASINGLY USE A MOBILE-FIRST BUSINESS MODEL, THE THREAT TO ANY INDUSTRY USING THIS WILL INCREASINGLY COMPRISE MOBILE ATTACKS.

The threats within the mobile landscape are compounded by the use of employees' own devices and apps.

The entire threat matrix of mobile working is a complicated and overlapping one which links connections, apps, and the devices themselves.

Mobile attack vectors include both internal (insider) as well as external threats. In this respect, the type of security threats that affect mobile devices mirror the same threats that an organization sees across non-mobile IT systems. Data exposure, ransomware that locks devices, and theft of patient records are as prevalent on mobile devices as they are on traditional computers. Mobile security attacks equate to lost health data: the "IBM X-Force Threat Intelligence Index 2017" [12] placed healthcare in the top 5 most targeted industries. A 2018 Cisco report on security threats found that mobile security threats were the number one most difficult risk for organizations to defend against [13].

MOBILE SECURITY THREATS ARE THE NUMBER ON MOST DIFFICULT RISK FOR ORGANISATIONS TO DEFEND AGAINST

Let's look at some of the specifics of mobile threats against organizational mobile users across three layers:

DEVICE LEVEL

Mobile devices are vulnerable to the same threats as the desktop or laptop. Mobile malware is proliferating as we move to a more mobile-first environment. Mobile trojans and ransomware are of particular concern for the mobile-led healthcare organization. In Q3 of 2017, Kaspersky Lab detected 1,598,196 instances of mobile malware - 120% up from the previous quarter [14].

Pre-installed malware is also a concern for healthcare. The idea that malware is usually installed accidentally by the user is no longer valid: this is evidenced by the recent case of a telecoms company who bought in 36 Android devices that were infected with malware - the infection having come in via someone with administrator privileges [15].

MOBILE LEVEL

International Mobile Subscriber Identity (ISMI) is being used in the form of an ISMI-catcher which is a malicious (rogue) cellular transmitter that uses device surveillance to eavesdrop and/or spam mobile devices.

An ISMI-catcher, also known as a 'stingray' is commonly used by law enforcement to detect illegal activities, but the same tech is also being used by cybercriminals as a way of performing a mobile-based Man-in-the-Middle attack.

APP LEVEL

Mobile app security has long been known to be a general issue. In a report by WhiteHat Security [16] into mobile apps, they found that 90% of Android apps they tested had a vulnerability that allowed private data to be exposed.

The same report found that 28% of health apps had serious security vulnerabilities. IOS has fared somewhat better with 30% of apps having a security vulnerability and around 18.8% using no encryption, thus allowing sensitive data to be communicated with no protection.

90% OF ANDROID APPS TESTED HAD ALLOWED PRIVATE DATA TO BE EXPOSED

KASPERSKY LAB DETECTED 1,598,196 INSTANCES OF MOBILE MALWARE

Public vs. Private Messaging Apps

The security of mobile devices and mobile apps is often a case of deciding which type of app to choose. There are a number of messaging apps available, but some are more public than others. This design remit impacts the level of security offered by the app and needs to be factored in when making a choice about which to employ in your organization.

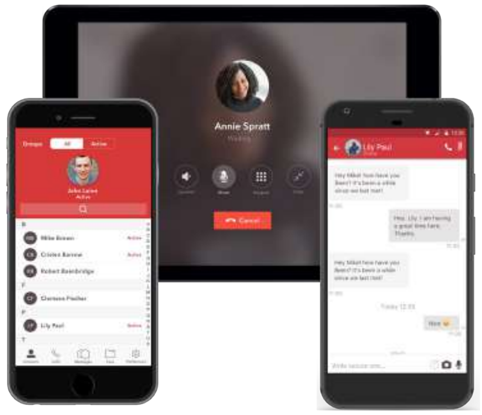
PUBLIC MESSAGING APPS:

Confidentiality is a key concern for healthcare providers. Patient information and personal data are shared between practitioners as part of their day-to-day communication. One area causing concern in healthcare is the use of consumer or patient-facing messaging apps for healthcare communication or work-related information. A survey of over 300 companies, carried out by Ovum [17] into the use of messaging apps, found that 65% of respondents were concerned over security issues when employees used 'chat apps' like WhatsApp for work. Worryingly, over 50% of respondents were unable to monitor this use. Public-facing apps like WhatsApp are becoming common in healthcare. In a recent survey by a doctor into the use of the messaging app in her own hospital, she found that 30% of doctors used WhatsApp for work-related communication [18].

Issues found with the implementation of encryption in apps like WhatsApp make the use of public messaging apps in healthcare dubious. A group of security researchers from Ruhr University Bochum in Germany [19] have described flaws in encrypted messaging apps such as WhatsApp, Signal, and Threema. These flaws allow external parties to insert new people into private messaging groups - something that would have serious repercussion if using those apps to communicate on patient care. A simple act like this, within a highly controlled industry like healthcare, could constitute a breach of highly confidential patient data.

PRIVATE MESSAGING APPS:

Private messaging apps can be used as an alternative to public messaging apps. These apps are built specifically to solve the issue of security when communicating via mobile app. Private messaging apps offer a closed system which is specifically built for collaboration and messaging within a secure environment, using encryption. Only the people with access rights can access the communications. There are a number of consumer apps that provide some level of protection, but there are also enterprise-focused apps which provide military grade protection along with extended collaboration features.



ROUND-UP OF PRIVATE VS. PUBLIC MESSAGING APPS

	Public messaging	Private messaging
DATA PROTECTION	No encryption of data, with some exceptions. For example, WhatsApp utilizes encryption, however if an employee leaves an organization there is no way to easily retrieve messages which could contain sensitive information.	Encrypted messaging and control of messaging.
LACK OF CONTROL	Lack of control of public apps means that company messages can be mixed with personal messages - this can cause fuzzy boundaries and potential for sensitive information exposure.	Ability to define roles and access control to ensure company messages are kept internal to the organization.
APP SECURITY	More open to malware attacks.	Protected against vulnerabilities and have regular updates.
AUTHENTICATION AND ACCESS CONTROL	Usually no authentication required for access, or poorly applied - for example 1234 code-based without underlying controls offered through policies.	Ability to control access using passwords that can be managed via policies that comply with standards such as NIST.
DATA PRIVACY	No emphasis on Privacy by Design (PbD) principles in app design. External users can be added to private groups ad hoc (WhatsApp, for example, has an informal approach to groups with users able to be added at will, putting communications at risk of exposure) (20). Public messaging apps may not comply with privacy laws such as HIPAA and GDPR.	Well designed apps will be built to PbD standards. Full control over groups and messaging is inherent in the design of the app.
SECURE COLLABORATION	Usually no extended functionality, and insecure even where features offered.	Secure collaboration across a number of channels of communication, often including file sharing.
INTEGRATION WITH EXISTING INFRASTRUCTURE	Not designed to integrate easily with existing infrastructure - at risk of becoming part of Shadow IT.	Ability to easily integrate with existing infrastructure. For example, seamless integration with existing Private Branch Exchange (PBX) and the re-use of existing healthcare IT systems.

Compliance for Third Party Mobile Messaging Apps

Compliance accommodates the changing threat landscape, with updates in areas such as the EU's General Data Protection Regulation (GDPR), HIPAA in healthcare, and PSD2 in the financial space.

The mobile health-focused organization could be adversely impacted by the use of mobile messaging unless specific compliance-led targets are adhered to. In a report by Lookout, they found that 84% of IT executives expected GDPR compliance to fall short when data was accessed via a mobile device [21]. The same report found that 63% of employees accessed customer, employee or partner data from a mobile device.

Privacy is under intense scrutiny, now more than ever, and is a particular area of mobile app usage that has issues. This was evidenced in the case of Consumer Financial Protection Bureau vs. Dwolla [22]. The payment platform Dwolla misrepresented the level of data security they offered for personal data and were found not to fully test the security of their mobile apps. Design of messaging apps needs to take privacy seriously and build in a number of privacy features across the layers.

Data security too is a risk factor in data access and sharing. In the Lookout report they found poor employee behavior regarding app usage. This included employees downloading apps from unapproved stores, using unsafe links, and failure to install security patches.

All of these issues fall outside of the expectations of compliance requirements affecting all industry sectors.

THREE TIPS TO SECURING MOBILE DEVICES

Ensuring mobile security is an essential part of a comprehensive approach to creating a secure enterprise. The extension of an enterprise's security strategy in the mobile arena allows it to ensure a true end-to-end approach to securing company data and protecting both its own and extended user base data. Some tips for mobile security success include:

MOBILE DEVICE MANAGEMENT (MDM)

MDM is a fundamental control strategy for the mobile enterprise. Using an MDM system can help you to identify endpoints across all devices, including smartphones. It can also allow you to put policies such as access control and patch management in place.

APPLICATION BLACKLISTING

A Ponemon Institute study [23] found that 60% of respondents had suffered a data breach as a result of an insecure mobile app. It is vital that mobile app installs are monitored and controlled.

USE SECURE MESSAGING APPS

The Open Web Application Security Project (OWASP) regularly creates a list of the top ten [24] greatest threats against mobile devices. In their 2016 analysis, they placed data security issues as the most pressing. These security threats include:

- Insecure data storage
- Insecure communication
- Insecure authentication
- Insufficient cryptography

This magic quartet is intrinsic to the robust design of a secure messaging app like Adeya.

Part Two:

Mobile Messaging in the Healthcare Sector

Healthcare was in the spotlight in 2017 over a number of very high profile cybersecurity issues including the massive WannaCry ransomware attack.

WannaCry affected 20% of NHS trusts and infected 1,200 pieces of diagnostic equipment [25]. There are a number of reasons why healthcare is a target for cybercrime: there is a lot of valuable data used by the industry; confidential patient data as well as intellectual property (IP) such as experimental procedures, drug trials data, and so on. Additionally, the industry, while still depending on some legacy technology like paging systems, is often an early adopter of new technology, such as smart devices, mobile phones, and the Internet of Things. In the industry, mobile-based healthcare or 'mhealth' is showing major growth, driven by data being shared across healthcare providers, patients, and business associates. With statistics showing that 25% of patients missed a referred appointment because records did not reach a provider in time, a mobile app can turn a smartphone into a medical tool [26].

Many countries, like the USA and UK, are pushing for mobile based patient engagement to create better physician-carer-patient interactions for better patient outcomes. On the back of these expectations, the mobile health apps market is expected to be worth almost $112 billion by 2025, growing at a massive CAGR of almost 45% [27].

The impact of cybercrime on the health industry is far reaching and costly. In the Ponemon Institute "2017 Cost of Data Breach Study" [28] they found that healthcare had a higher data breach cost than any other sector; the average cost per lost record being $380. Healthcare records themselves are valuable commodities. In a recent expose by DataBreaches.net, they found healthcare record data on sale on the dark web for around $300 per record [29].

Organizations like the World Health Organization (WHO) [30] have published a checklist of recommendations and best practice use of mHealth and mobile apps. This includes advise such as ensuring appropriate training in the use of health apps and the use of measures to protect the privacy and confidentiality of participant identity and health information that also cover compliance such as HIPAA. In an effort to redress the balance of security in health data communications, compliance and regulatory frameworks are being tightened to help safeguard patient and IP data. Healthcare frameworks, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the EU's GDPR, place pressure on healthcare organizations to ensure that the right level of data protection is applied. These regulations are often nuanced and have multiple touch points across the data lifecycle.

AS WE HAVE SAID, HEALTHCARE IS A HIGHLY TARGETED INDUSTRY. TO FIND OUT WHERE THE WEAKNESSES IN THE INDUSTRY WERE, THE PONEMON INSTITUTE CARRIED OUT A STUDY INTO THE SPECIFIC PRIVACY AND SECURITY ISSUES FACING THE HEALTHCARE INDUSTRY. THE STUDY FOUND THAT 90% OF RESPONDENTS HAD EXPERIENCED A DATA BREACH IN THE TWO YEARS LEADING UP TO THE STUDY, WITH 45% OF THOSE EXPERIENCING FIVE OR MORE ATTACKS (20). EXAMPLES OF HEALTHCARE CYBERSECURITY ISSUES INCLUDE:

INSIDER THREATS: A Verizon report found that 58% of protected health information (PHI) were affected by insider breach. However, not all of these insider threats were malicious. Around 34% were down to human error and 30% to misuse/mis-delivery. Use of stolen credentials was also a major issue identified in the report [31].

As sensitive data moves onto an mHealth platform and messaging apps are used to communicate between patient and caregiver, the likelihood is that insider threats will follow that thread. Mobile messaging apps need to have robust access control policies and authentication measures. Auditing, and rules like geolocation controls are also vital in the war against insider threats.

SECURE MOBILE MESSAGING SOLUTIONS: One of the mainstays of good medicine is good communication. In a modern context, where over 80% of physicians use smartphones at work, communicating via a mobile messaging app offers convenience for a heavy workload. But mobile messaging isn't just about communicating with patients, it is also about collaborating with colleagues. Healthcare presents mobile messaging apps with the challenge of protecting massive amounts of patient data. During research carried out in University Hospital Limerick, Ireland, they found that there was ubiquitous use of messaging apps like WhatsApp in the work context [32]. The report goes on to say that "95% of respondents feel that it is 'safer for patients' if everyone on the team uses an instant messenger". In another report based on U.S. hospital staff, they found that 65% of co-workers shared patient data via SMS text message and 33% using WhatsApp [33] However, the security of the app is a major concern and the best practice in messaging apps use is highlighted in the report.

Mobile messaging apps offer the healthcare sector many benefits. These messaging apps can be used to speed up the sharing of patient data to improve patient outcomes. They can provide better patient interaction with the health service and help to build better patient-caregiver relationships. Mobile messaging can also offer a more seamless and faster way for teams to collaborate. However, they must be secure and offer granular

Unless the apps are secured using reliable mechanisms including encryption and robust authentication, patient data will be exposed to attack. In addition, groups used for co-worker collaboration must have robust access control mechanisms attached.

DATA PROTECTION AND MOBILE SECURITY IN HEALTHCARE: The security of protected health information (PHI) is a serious issue in healthcare. Health record compromises often make headline news. But the loss of health data is not always malicious, as was the case when half a million health records in the UK NHS went missing [34]. However, as already discussed, hacking and insider threats also pose a major threat to health data. Malicious or otherwise, as healthcare embraces mHealth, mobile apps will become a target point for cybercrime.

Healthcare has to abide by a variety of regulations depending on jurisdiction. Data protection spans many vulnerable areas of mobile data and as mobile apps and secure messaging become ubiquitous, the data flow across these apps needs to be secured but still collaborative.

RANSOMWARE: Healthcare institutions and organizations are a favorite target for ransomware attack. Mentioned earlier was the WannaCry attack that had a massive impact on the UK NHS, causing some hospitals to close wards and delay operations. But ransomware hits healthcare across the globe. The number of ransomware attacks against U.S. healthcare organizations in the year 2016-2017 increased by 89% [35].

Ransomware is increasingly affecting mobile devices, up 250% in Q1 of 2017 [36]. Mobile messaging apps used in healthcare need to be built to security standards that make them robust against vulnerabilities. Messaging apps also need to have regular updates and patches to keep up to date with changing security threats.

COMPLIANCE AND REGULATION OF DATA SECURITY IN THE HEALTHCARE SECTOR

Data security compliance in healthcare is currently a patchy set of jurisdiction-led regulations. As a general guide, healthcare compliance standards are usually built around the audit of processes and procedures used to protect data and respect the privacy of patient information. In the healthcare industry a number of focused regulations and laws exist. These include:

IN THE USA:

Health Insurance Portability and Accountability Act (HIPAA):

HIPAA is a law in the USA that has wide coverage of health-related activities. Under the umbrella of HIPAA are several rules which are highly pertinent to security and privacy of health records:

PRIVACY RULE:

This is a set of national standards that ensure that patient data is under the control of the patient. It sets out patient rights on the use of this data and limits the conditions on the use of patient data.

SECURITY RULE:

This sets out the national standards on how to store and transmit patient data. It sets out methods to establish the confidentiality, integrity, and availability of ePHI. It covers both physical and digital protection methods to secure PHI.

OMNIBUS RULE:

This rule was an update to HIPAA. It was a modification of HIPAA to allow for the implementation of certain other rulings in a related act; the Health Information Technology for Economic and Clinical Health (HITECH). HITECH was designed to offer a framework for securing electronic health records. Omnibus is a mechanism for extending the privacy and security expectations of HIPAA/HITECH to the wider healthcare ecosystem. This includes any firm that is a 'business associate' and thus processes health data.

BREACH NOTIFICATION RULE:

This rule requires that any HIPAA covered entity must inform the affected individuals, the U.S. Department of Health & Human Services (HHS), and under certain conditions, the media, if unprotected PHI suffers a breach. The breach of PHI from 500 or more individuals is posted to the publicly accessible, OCR website [37].

IN THE UK:

The UK has a complicated system of multiple healthcare 'trusts', and data-sharing between trusts is proving problematic. The Caldicott report "Review of Data Security, Consent and Opt-Outs" [38], is the third exploration commissioned by the UK Government. The report focuses on trust and data security. The UK Government released a reply to this, "Your Data: Better Security, Better Choice, Better Care" [39], which encourages the use of patient-centric consent models around data sharing. As this new structure pans out, UK health organizations come under the compliance umbrella of the NHS Information Governance Statement of Compliance (IGSoC).

IN AUSTRALIA:

The Healthcare Identifiers Act (2010) (HI Act):

The HI Act is used in combination with three other frameworks:

- Healthcare Identifiers Regulations 2010
- Privacy Act 1988
- Australian Privacy Principles

Together they direct and limit the use of health identifiers. In doing so, they set out best practice expectations around data security and also impose penalties on health data breaches [40].

OVERARCHING COMPLIANCE FRAMEWORKS AND HEALTHCARE

The EU and a number of associate countries including Switzerland, will be expected to abide by the General Data Protection Regulation (GDPR) from May 25, 2018. The GDPR is a set of regulations that control the use of personal data.

The regulations set out a number of 'data subject rights' which strengthen the rights of the individual when an organization processes their data. These rights include the 'right to be forgotten, 'right to restrict processing of data, and the 'right to access data' as well as several others. Consent is a central pivot point in the GDPR and user consent must be explicitly sought when processing data, including health-related data.

The GDPR is a wide-scope regulation which covers the processing of personal data. In terms of the healthcare industry, the GDPR is about building the ethos of Privacy by Design (PbD) into all structures that handle and process patient data.

In the case of countries like Finland, Switzerland, and the UK, the current laws covering data protection across a number of industries, such as the Federal Act on Data Protection (FADP) in Switzerland and the Data Protection Act (DPA) in the UK, will be updated and aligned with the GDPR.

In the GDPR, definition of what constitutes personal data is that which "means any information relating to an identified or identifiable natural person"- for example name, address date of birth, etc. (41). The GDPR also includes various other health-related data in the definitions of what personal data is. There is a 'special' category for personal data which includes: genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a natural person's sex life or sexual orientation.

Special category data have additional restrictions on the processing and handling of these data. In addition, certain considerations such as privacy of the data of deceased persons are not specifically exempted under the GDPR. This data will need to be considered when carrying out a health data related privacy impact assessment.

The healthcare sector is embracing the use of messaging apps to enhance team collaboration and improve patient-caregiver communications. However, the use of public messaging apps for these communication channels can cause serious privacy and security gaps. To meet GDPR and other compliance requirements and mitigate data security risks, these apps must meet the security and privacy needs of the sector.

Private messaging apps have been designed to ensure two key criteria are met:

CONTROL:

Private messaging apps are built to enable secure collaboration and provide robust access control measures to keep conversations isolated. This level of control can ensure that highly sensitive patient data and IP data, are protected. The issue of misuse and misdirection of such data is minimized, if not eliminated.

COMPLIANCE:

Public apps will not have the level of security and privacy needed by the healthcare sector for full data security compliance. Private, purpose-built apps will have Privacy by Design as a design remit. The privacy and security of sensitive patient data is paramount in the app design.

Part Three:

Healthcare Sector Use Case

The following is a real-life use case of the Adeya messaging app used by a healthcare organization.

In this case, hospital staff were regularly using personal smartphones as a type of 'shadow IT' to improve on existing legacy communication technologies. This created a compliance issue within the organization. They had no control over the data sharing being carried out using personal mobile devices, yet still had to meet the stringent compliance requirements around patient data security and privacy. This case demonstrates how staff can use their own smartphones to securely communicate clinical information and discuss patient care, whilst staying within the regulation requirements of data security laws. It also shows how healthcare workers can create secure collaborative groups that can be used even when no Wi-Fi is available.

PROBLEM STATEMENT:

Hospital staff used existing mobile phones to communicate about patient care, etc. This was found to be a convenient and speedier solution for communicating information and as a way of circumventing traditional pager systems and email which were considered lacking in capability and speed.

Communication was carried out using SMS and publicly available messaging apps which were downloaded from public app stores. This created some serious compliance and security issues. The apps chosen were not designed for the type of data security needed to protect sensitive health data.

Extended security functions (e.g. management of group members) was not available using public messaging apps. They didn't fit the criteria for hosting data, i.e. on-premise or Swiss-based Cloud hosting.

RESOLUTION:

Adeya was chosen as the best solution to solve the hospital's secure communication needs by addressing these problems:

CONTROL: Adeya offered full end-to-end encryption of communications. This was a vital piece of the compliance puzzle. Groups had to be fluid, yet highly secure. Groups could be managed remotely and external users added/removed as the group required. Communication groups could be isolated and with controlled access to them - only authorized individuals could work in the communication groups.

NO WIFI: Adeya could offer the organization a way to still retain end-to-end encrypted messaging even when WiFi was not available.

FAMILIAR ENVIRONMENT: Hospital staff were able to use the Adeya app on their personal smartphone.

About Adeya

Adeya (ἄδεια): "freedom from fear" (Ancient Greek).

Adeya has long-standing expertise in building world-class security and mobile applications. We work with your organization to make sure that your communications are collaborative, and under your control. Adeya solutions are used across many industry sectors including healthcare, financial, government, and utility services. By offering both on-premise and Cloud-based solutions, Adeya can provide the exact requirements needed to ensure security, compliance, and control are handled in a cost-effective manner. Our products have been built to an exacting design remit to help with the digital transformation requirements of the modern organization.

SWISS + swiss made software

REFERENCES

1 **Statcounter**, *Mobile and tablet internet usage exceeds desktop for first time world-wide*: http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide

2 **Mordor Intelligence**, *Global Mobile Health (mHealth) Market*: https://www.mordorintelligence.com/industry-reports/mobile-health-market

3 **Ericsson**, *Ericsson Mobility Report 2017*: https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-november-2017.pdf /mobile-health-market

4 **HIMSS**, *2015 HIMSS Mobile Technology Survey*: http://www.himss.org/2015-himss-mobile-technology-survey-executive-summary?ItemNumber=41510

5 **Statistica**, *Number of mobile phone messaging app users worldwide from 2016 to 2021 (in billions)*: https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/

6 **The Radicati Group**, *Instant Messaging Statistics Report, 2018-2022*: https://www.radicati.com/wp/wp-content/uploads/2017/12/Instant-Messaging-Statistics-Report-2018-2022-Brochure.pdf

7 **Aruba Networks**, *Mobility, performance and engagement*: http://www.arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf

8 **Nursing Times,** *How mobile technology can improve healthcare:* https://www.nursingtimes.net/clinical-archive/healthcare-it/how-mobile-technology-can-improve-healthcare/5056269.article

9 **Business Wire,** *HRS PatientConnect Tablet Reduces Congestive Heart Failure Readmissions by 53%:* https://www.businesswire.com/news/home/20150408005312/en#.VTAcNPnF99L

10 **mHealth Intelligence,** *mHealth Study:* https://mhealthintelligence.com/news/mhealth-study-remote-monitoring-cuts-costs-hospitalizations

11 **RedHat,** *Gartner, Intel, Transforming Healthcare, 2016*

12 **IBM X-Force Threat Intelligence Index 2017:** https://www.ibm.com/security/data-breach/threat-intelligence

13 **Cisco,** *2018 Annual Cybersecurity Report:* https://www.cisco.com/c/en_uk/products/security/security-reports.html

14 **SecureList,** *IT threat evolution Q3 2017. Statistics:* https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/

15 **Checkpoint,** *Preinstalled Malware Targeting Mobile Users:* https://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

16 **WhiteHat Security,** *2017 Application Security Statistics Report:* https://info.whitehatsec.com/rs/675-YBI-674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf

17 **Ovum,** *Secure Enterprise Messaging in the Age of the Chat App:* https://ovum.informa.com/resources/product-content/secure-age-chat-app

18 **ThinkinCircle,** *Whatsapp and the NHS:* https://www.thinkincircles.com/whatsapp-and-the-nhs/

19 **Roseler,** *P., et.al., More is Less:* On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema, Ruhr-University: https://eprint.iacr.org/2017/713.pdf

20 **Financial Times,** *The perils of using WhatsApp at work:* https://www.ft.com/content/4fbf6c18-a501-11e7-b797-b61809486fe2

21 **Lookout,** *Finding GDPR noncompliance in a mobile-first world:* https://www.lookout.com/info/wp-gdpr-lp

22 **Consumer Financial Protection Bureau,** *Dwolla Inc.:* https://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf

23 **Ponemon Institute,** *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data:* https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

24 **OWASP,** *Mobile Top 10 2016-Top 10:* https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

25 **Digital Health,** *NHS trusts fail post-WannaCry cyber security checks:* https://www.digitalhealth.net/2018/02/nhs-trusts-fail-post-wannacry-cybersecurity/

26 **The Milbank Quarterly,** *Dropping the Baton:* Specialty Referrals in the United States: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3160594/

27 **GrandView Research,** *mHealth Apps Market Size:* https://www.grandviewresearch.com/press-release/global-mhealth-app-market

28 **Ponemon Institute,** *2017 Costs of Data Breach Study:* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

29 **DataBreaches.net:** https://www.databreaches.net/infant-social-security-numbers-are-for-sale-on-the-dark-web/

30 **WHO,** *New checklist published to help improve reporting of mHealth interventions:* http://www.who.int/reproductivehealth/topics/mhealth/mERA-checklist/en/

31 **Verizon,** *2018 Protected Health Information Data Breach Report:* http://www.verizonenterprise.com/verizon-insights-lab/phi/2018/

32 **BMJ Journals,** *WhatsApp Doc?:* http://innovations.bmj.com/content/early/2017/10/24/bmjinnov-2017-000239

33 **Skycure,** *Mobile Security Trends in Healthcare:* https://www.skycure.com/blog/mobile-security-trends-in-healthcare/

34 **BBC News,** *NHS misplaced half a million patient documents:* http://www.bbc.co.uk/news/health-39101489

35 **Cryptonite Press Release,** *2017 US Healthcare Breaches Involving Ransomware Increased 89% Year-Over-Year:* https://www.businesswire.com/news/home/20180105005054/en/2017-Healthcare-Breaches-Involving-Ransomware-Increased-89

36 **Securelist:** https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

37 **U.S. Department of Health and Human Services,** *Office for Civil Rights, Breach Portal:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

38 **National Data Guardian for Health and Care,** *"Review of Data Security, Consent and Opt-Outs", June 2016:* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

39 **Department of Health,** *"Your Data: Better Security, Better Choice, Better Care", July 2016:* https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

40 **Office of the Australian Privacy Commisioner:** https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-1-individual-healthcare-identifiers-compliance-obligations-of-private-healthcare-providers

41 **GDPR Article 4:** https://ec.europa.eu/info/law/law-topic/data-protection_en#page=33

ADEYA

ADEYA

α’’δεια: “freedom from fear” (Ancient Greek)

📍 Rue Saint-Louis 2,
Morges, Switzerland, CH-1110

☎ + 41 22 566 14 80

✉ contact@adeya.ch

www.adeya.ch