SAMSUNG

White Paper:

Securing Healthcare Apps

Keeping Patient Data Secure in the Mobile Healthcare Era

There's been a veritable explosion in the number of mobile apps being developed and used for health status tracking and health promotion over the past few years. Most of these apps contain personally identifiable information (PII), as well as protected health information (PHI), both of which are extremely valuable to identity thieves and other criminals. Yet until now, security has not been a major focus for mobile apps, particularly healthcare apps. But as mobile healthcare apps gain popularity, the risk of data theft is increasing. The ramifications, both monetary and otherwise, can be significant when patient data is compromised. This paper will discuss the critical issues surrounding this topic and look at what healthcare providers can do to significantly lessen the risks related to healthcare data stored on mobile devices.

About the Author:

Steve Kastin, MD, is a physician who has been involved with healthcare IT for over 20 years. He is currently the Chief Medical Officer at By Light Professional IT Services. Prior to that, he was Chief Healthcare IT Strategist at the U.S. Department of Veterans Affairs, as well as a Clinical Assistant Professor of Radiology at the NYU School of Medicine in New York City.

The views expressed in this white paper are those of the author, and should not be construed as an endorsement by the US Government or the US Department of Veterans Affairs.

The Proliferation of Mobile Computing and Mobile Health Apps

According to a 2015 study conducted by Kantar Media, 84 percent of physicians use a smartphone in their practice, while 56 percent use tablets.[1] Further, it's estimated that 81 percent of the world's mobile devices currently run on the Android operating system, and that this percentage will increase to 83 percent by 2019.[2] According to a 2015 report from the IMS Institute for Health Informatics, there are over 165,000 mobile health (mHealth) apps currently available.[3] A 2015 article in the Journal of Medical Internet Research claims that 58 percent of surveyed users had downloaded at least one healthcare app onto their phones.[4] And from a business perspective, healthcare apps are expected to represent a $26 billion market by the end of 2017.[5] Needless to say, the patients your organization cares for will be using one or more mobile healthcare apps in the near future, if they aren't already.

And patients aren't the only ones using mobile apps for healthcare. As a result of government incentives, the vast majority of healthcare organizations now utilize electronic medical records. As in other industries, healthcare providers are increasingly mobile and need to be able to access patient information at any time, from any location, on any device.

As a result of this increasing mobility, healthcare organizations are faced with a choice: They can either institute a "bring your own device" (BYOD) policy, or provide mobile devices to their employees. Sometimes, to prevent employees from having to carry two separate devices, these corporate devices contain a "personal" partition, a strategy referred to as "corporate-owned personally enabled" (COPE). Each strategy brings its own challenges, as mobile devices present multiple issues surrounding security and privacy. This is especially true when a single device is used for both corporate and personal purposes.

Medical apps are "hot": According to a 2015 report, there are over 165,000 "mHealth" (mobile health) apps currently available.

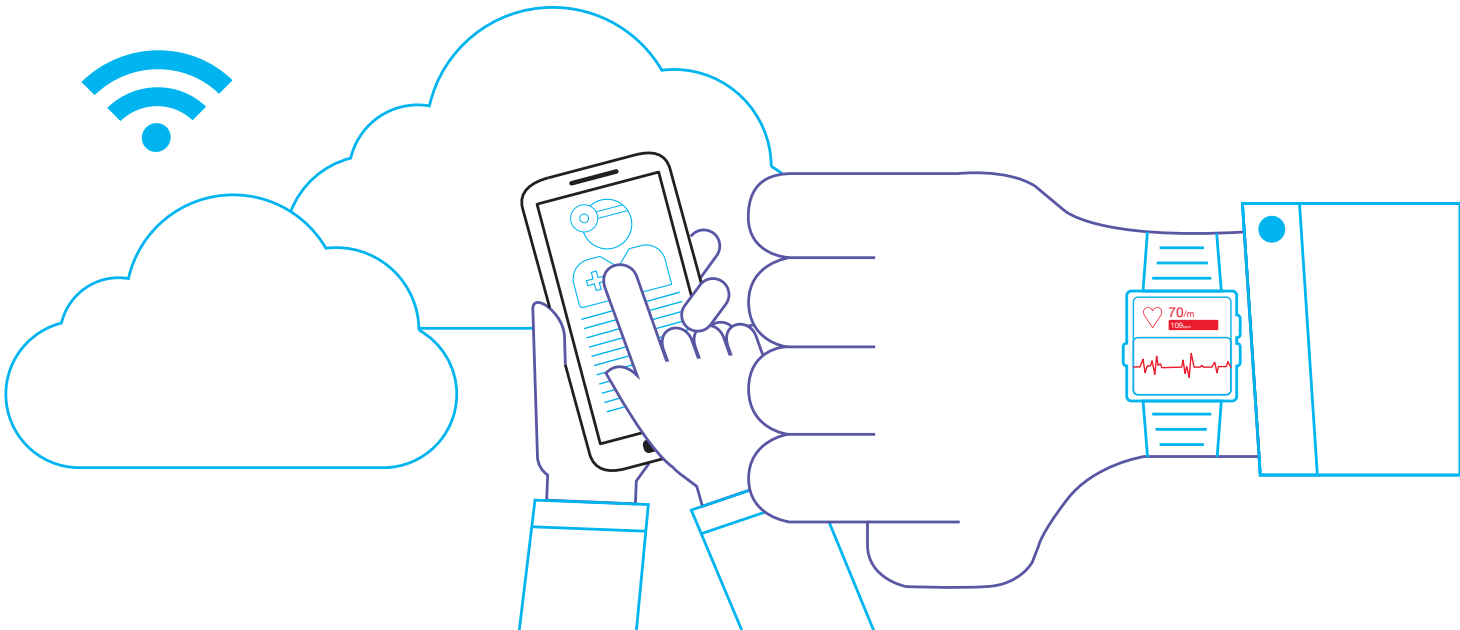
Protecting Data in the Age of Personalized Medicine

More and more patient data is available each day for healthcare workers to assimilate. We've heard recently about the concept of big data in medicine, both in terms of the current reality (the huge amount of patient data already being generated) and the promise — to be able to analyze all of that data, from multiple sources, in order to be able to make more intelligent decisions about patient care.

Another concept attracting increasing attention these days is "personalized medicine" (sometimes also called "precision medicine"). Everyone reacts to diseases, therapies and medications differently. We know that there are differences based on age, gender and race, among other factors, but these are only broad generalizations. With the knowledge that every individual is a bit different, and that these differences are based significantly on genetic and epigenetic factors, the Obama administration created the Precision Medicine Initiative[6] to foster the use of individualized care based on a person's unique attributes.

Determining the best way to treat a patient for a given problem often starts with knowledge of the individual's genetic makeup, which involves vastly more data about each patient than was ever available (or needed) before. This data then needs to be married with data (much of which is yet to be discovered) about the exact response to each given treatment based on a given genetic makeup. Furthermore, environmental and behavioral factors can also influence the clinical efficacy of treatments. We may discover, for example, that a given drug treatment works better in a warm climate than in a cold climate, all other factors being equal. Or we may find that a given treatment is effective (or much more effective) only when combined with some minimum amount of daily exercise. So, in order to proactively understand which treatments to try and how effective they might be, we need data — lots of data — on patients' behavioral and environmental factors. And we'll likely need this same data to monitor ongoing patient compliance with treatment regimens. (It's worth noting that the Precision Medicine Initiative appreciates that patient privacy and data security are critical to the success of this initiative, and have recently published their Data Security Policy Principles and Framework.[7])

Where will we get all the behavioral and environmental data that enables personalized medicine? The answer is from a multitude of sensors both in the patient's environment (e.g., in their home) and on the patient's body (e.g., from wearables). There are already hundreds, if not thousands, of such devices available on the market. In order to be useful, all of this collected patient data will need to be transmitted or made available to a healthcare provider. Information protection on these sensors, and during the transmission process, is a topic for another discussion, but it's certainly a critical issue that must be dealt with. Data from these sensors, especially wearables, is generally routed through a smartphone or other mobile device. Therefore, it's imperative that sensitive data be properly protected on these devices.

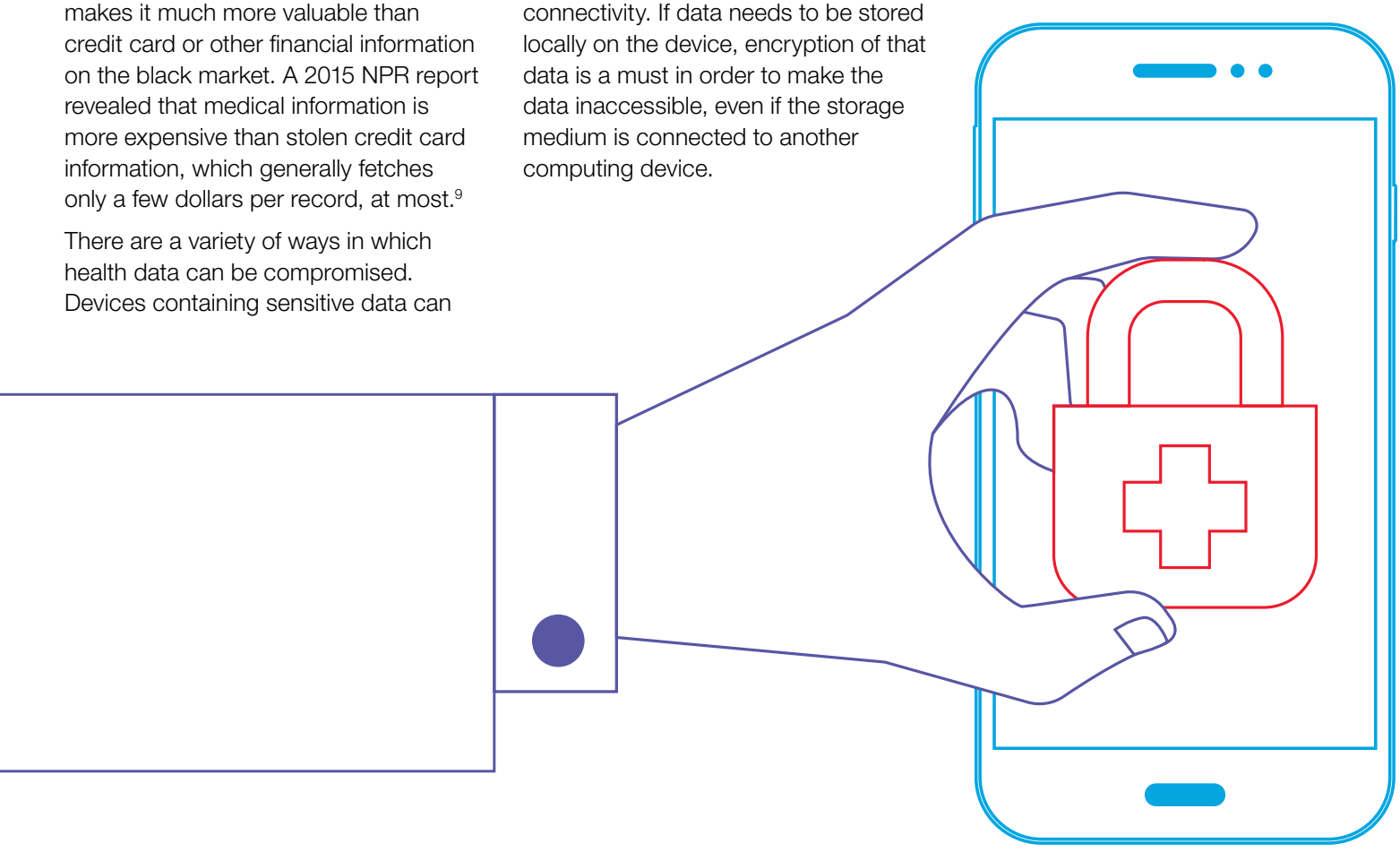


Medical Data Breaches Prove Costly

It seems that not a day goes by without a news story about medical data being compromised in some way. According to Forbes, in 2015 alone, there were 253 known data breaches that exposed over 112 million patient records to theft.[8] Data breaches include Anthem Healthcare (over 78 million records), Premera (11 million records), Excellus (10 million records) and many others. These breaches occur frequently because medical data is an especially lucrative target. If a credit card number is compromised, the bank simply cancels that number and issues a new credit card, and the stolen number may only be usable for minutes or hours. But if your name, address, date of birth and medical information is stolen, there's no way to change it. It's usable forever. The comprehensive and unchanging quality of medical data makes it much more valuable than credit card or other financial information on the black market. A 2015 NPR report revealed that medical information is more expensive than stolen credit card information, which generally fetches only a few dollars per record, at most.[9]

There are a variety of ways in which health data can be compromised. Devices containing sensitive data can be stolen. With the increasing use of mobile devices, thefts are more frequent, since the devices are more portable and generally are not physically locked down. Mobile devices can also be lost, which presents just as much of a risk for unsecured data as an intentionally stolen device. Devices can be stolen primarily for the value of the hardware, or it may be the data residing on the device that's being targeted. Theft of a device may even be incidental to a larger theft, such as the theft of a car in which a tablet or laptop is left. But in any of these scenarios, if the data is stored locally on the device, it's gone. Therefore, one strategy to consider is eliminating the local storage of any sensitive PII or PHI data on the device. Of course, the downside of this strategy, especially for mobile devices, is the requirement for "always-on" connectivity. If data needs to be stored locally on the device, encryption of that data is a must in order to make the data inaccessible, even if the storage medium is connected to another computing device.

Malware is an increasing concern: According to an article in Forbes, in 2015 alone, there were 253 known data breaches exposing over 112 million patient records to theft.



Mitigating Threats From Within

Another data security risk comes from insider threats, which can be broken down into two categories:

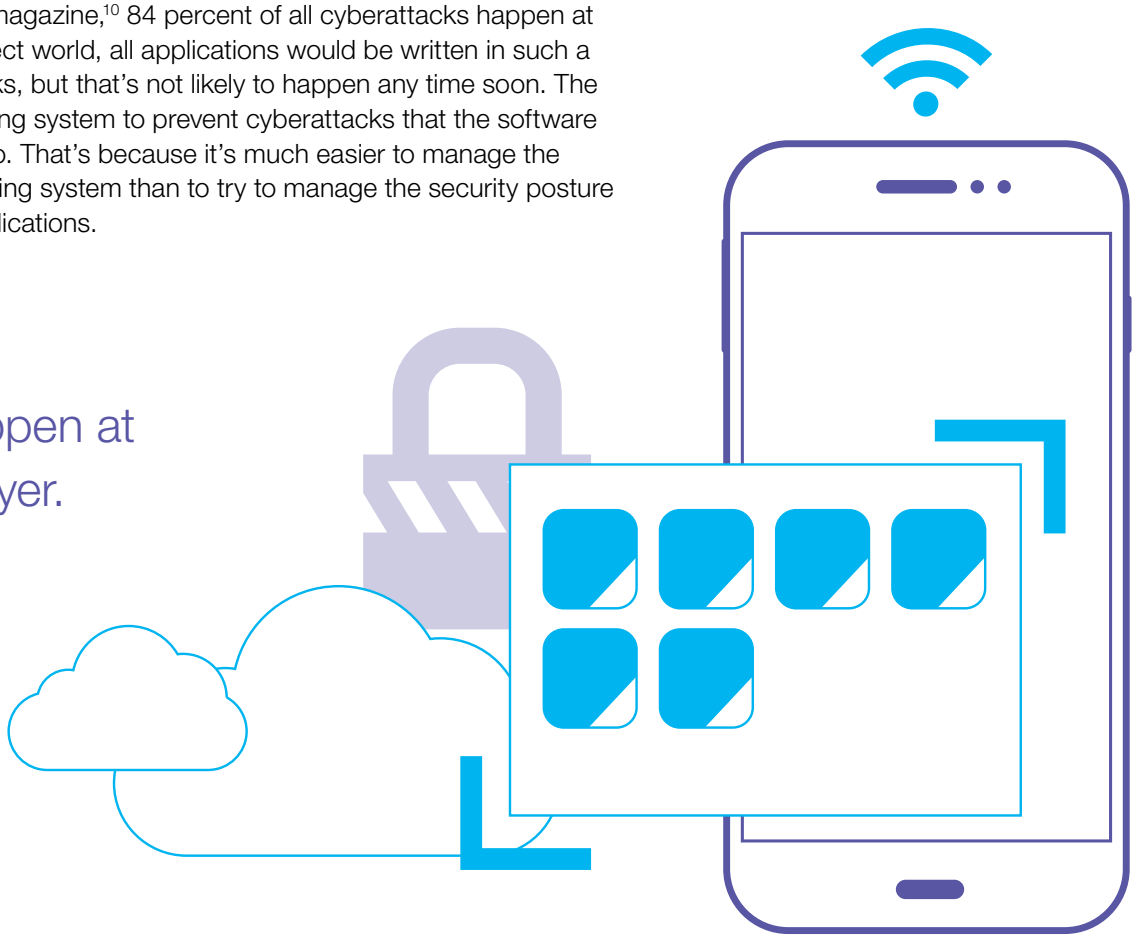
1. **Unintentional Threats:** These come from well-meaning employees divulging information when (and to whom) they shouldn't, often in the name of trying to help a patient or the organization. It also involves issues such as employees using weak passwords or writing down passwords where they can be seen. These kinds of threats can be lessened through good initial information security training, repeated at frequent intervals.

2. **Intentional Threats:** Another type of insider threat is the malicious employee who's out to make money, or simply has a grudge against the organization or a specific patient. All the training in the world won't help with this type of threat. Instead, providers must protect against this kind of breach by implementing ongoing data monitoring practices to detect exfiltration of sensitive data. These strategies can include the disabling of writing to optical media or other mass storage devices, scanning all outgoing email traffic for sensitive data and using behavioral analysis that detects sudden changes in computing behavior.

External Threats and the Advent of Ransomware

The types of threats we hear the most about are external. Attacks can target the hardware itself, the operating system or the application software. According to a March 2015 article in Forbes magazine,[10] 84 percent of all cyberattacks happen at the application layer. In a perfect world, all applications would be written in such a way as to prevent these attacks, but that's not likely to happen any time soon. The solution is to utilize the operating system to prevent cyberattacks that the software by itself would be vulnerable to. That's because it's much easier to manage the security posture of one operating system than to try to manage the security posture of thousands of individual applications.

84 percent of all cyberattacks happen at the application layer.



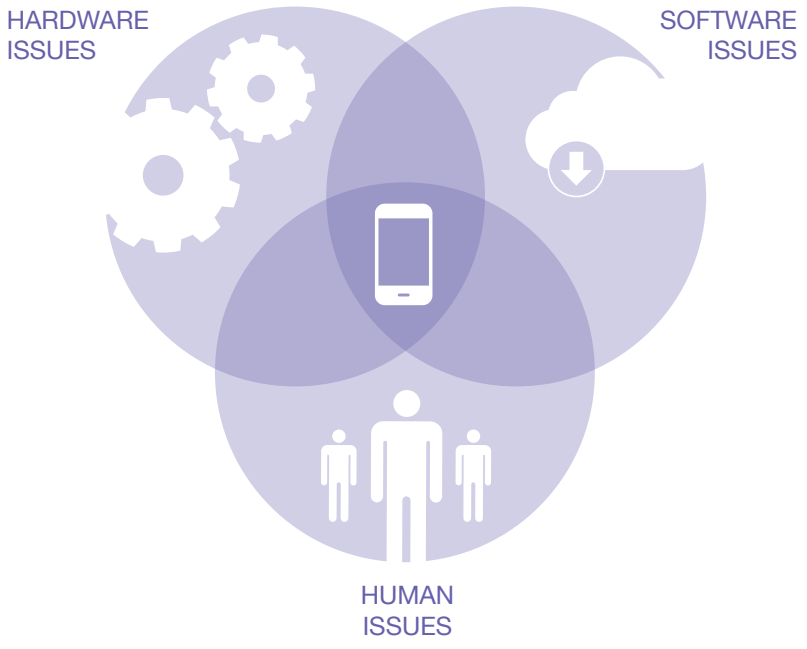
A Multilayered Approach to Ransomware

Most operating systems aren't designed to protect software at the application layer. Historically, hacks occurred via brute force password cracking, or perhaps through in-person or phone-based social engineering in order to obtain access. Nowadays, it's much more commonly achieved using malware designed to steal legitimate access credentials. In 2013, Juniper Networks estimated that mobile malware threats were increasing at a rate of 614 percent, up from 155 percent the previous year.[11] Phishing and malvertising are among the most common types of malware used for this purpose.

A newer trend is the use of "ransomware," in which an individual's or an organization's files are encrypted by malware, and the victim is required to pay a ransom to get the files decrypted. Since the beginning of 2016, we've seen ransomware attacks on Hollywood Presbyterian Hospital, several hospitals operated by MedStar Health in Maryland, Methodist Hospital in Henderson, Kentucky, three hospitals in California owned by Prime Healthcare and King's Daughters' Health in Indiana, among others. And if an attacker has the access to encrypt your files, they also have the access to read your files — unless you've encrypted them yourself. So, while ransomware is often viewed "only" as extortion and denial of service, it could also very well involve the compromise of sensitive health data.

Although the ideal scenario is to prevent any unauthorized access to your systems, a more realistic goal should be to minimize both unauthorized access and the amount of damage that can be done if it occurs. Therefore, it's important to implement strategies such as limiting the number of users with administrative rights and ensuring that those accounts with administrative rights don't also have email access. Requiring multifactor authentication (for administrative accounts, at a minimum, but ideally for all accounts) will also help, since attackers who gain access to passwords would also need access to the other factor(s) needed for login.

To minimize unauthorized access to your accounts, security needs to be multilayered. It's not enough to address only hardware issues, software issues or human issues. In order to optimize security, all three areas need to be addressed.



Android Security Gets an Upgrade

Although Google has always implemented a multitiered security model (including application sandboxing) and security services provided by Google Play services, Google has recently made significant improvements in Android security, including:

- Enabling deployment of full disk, block-level encryption
- Expanding the use of hardware-protected cryptography and removing older, exportable cipher suites
- Securing the Linux kernel by requiring SELinux (Security-Enhanced Linux) in full enforcing mode, which requires policies in an environment of Mandatory Access Controls (MAC)
- Incorporating secure inter-process communications (IPC)
- Implementing vulnerability exploit mitigation with ASLR (Address Space Layout Randomization)

Legal and Business Considerations

How people treat their own data (including health data) is often very different from how healthcare organizations are required to treat their data. An individual may not be aware of the risks they're exposing their personal data to, but even if they are, they may elect to accept those risks in the name of convenience. Healthcare organizations don't have that luxury. Healthcare data on patients and clients must be protected in compliance with HIPAA, Joint Commission requirements and a variety of other laws, including the Genetic Information Nondiscrimination Act (GINA), as well as state and local laws.

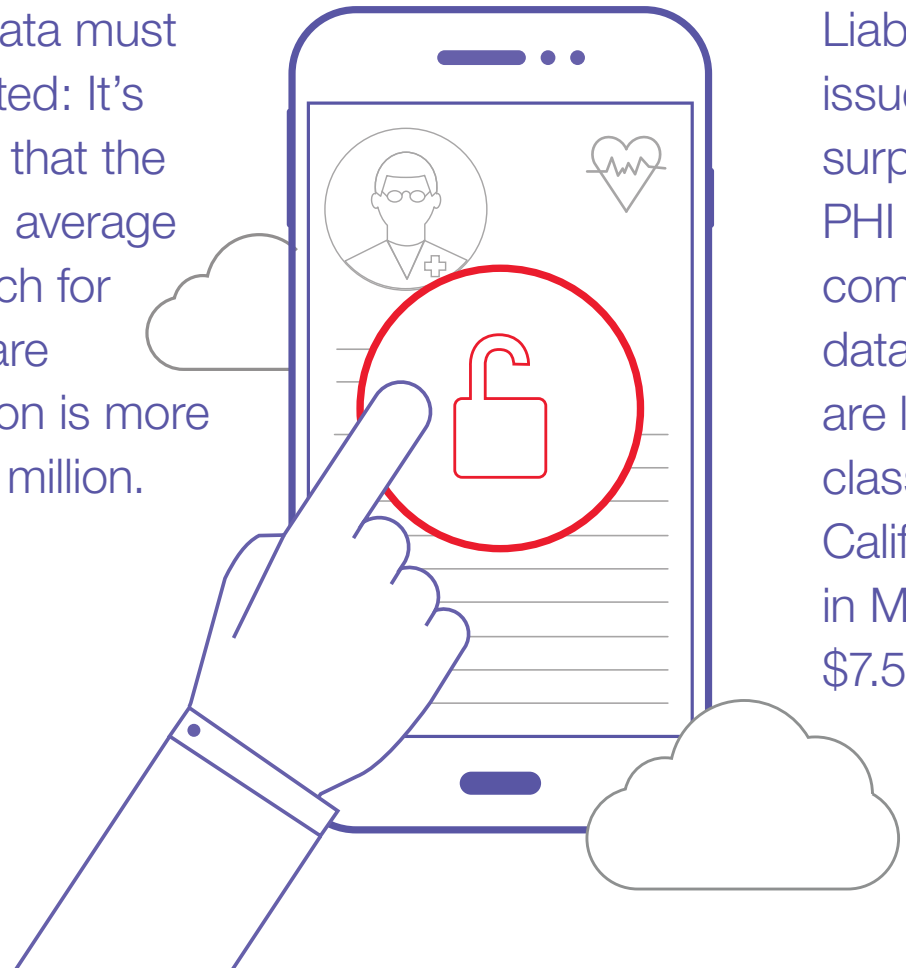
But with the rise in patient-generated data, these lines have blurred. Once health data has been transmitted from individuals to healthcare providers, those providers have a responsibility to protect that data in the same way they would protect internally generated data. In effect, consumer data is becoming protected health data.

The Ponemon Institute estimates that the cost of an average data breach for a healthcare organization is more than $2.2 million.[12] This includes not only the cost of data recovery and system remediation, but also the cost of credit monitoring for patients/clients. An additional factor to consider is the potential for government fines due to HIPAA violations, especially in light of two September 2015 studies[13,14] by the Department of Health and Human Services (HHS) Office of the Inspector General that called on the HHS Office of Civil Rights (which oversees HIPAA) to strengthen its enforcement activities.

In addition to the "hard" costs described above, a data breach will invariably cause reputational damage to your organization, which is likely to negatively impact business. Business losses include lost revenue and the cost to repair the organization's reputation.

Perhaps unsurprisingly, when PHI and PII are compromised due to a data breach, patients are likely to sue. This has been seen in a number of data breaches, including a class action lawsuit against St. Joseph Health in Irvine, CA that was settled in March 2016 for $7.5 million.[15]

Medical data must be protected: It's estimated that the cost of an average data breach for a healthcare organization is more than $2.2 million.

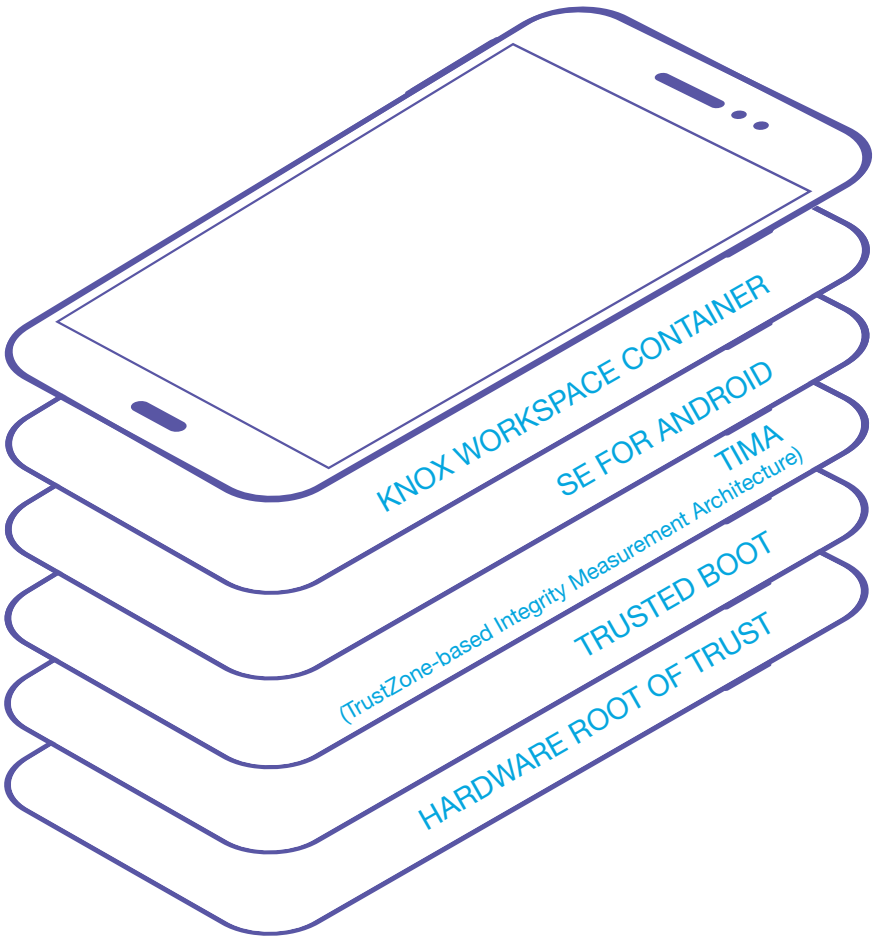


Liability is also an issue: Perhaps not surprisingly, when PHI and PII are compromised due to a data breach, patients are likely to sue. A class action lawsuit in California was settled in March 2016 for $7.5 million.

Preventing a Mobile Data Breach in Your Organization

Given that almost every healthcare organization will soon be using mobile apps, that malware is dramatically on the rise and that the repercussions of a data breach are so significant, what can you do to lessen the likelihood of a costly and damaging data breach involving mobile devices?

1. **Device Security:** First, it's important to understand that not all mobile devices are created equal. Not all hardware is equally secure, even if it has the same basic operating system, configuration, applications and the same use characteristics. Ideally, your device should provide "platform integrity" which requires that:
   - The hardware should ensure that no changes have been made to it and that it's operating in the expected manner
   - The boot process shouldn't be able to be subverted, either by the addition or deletion of approved software
   - The device provides hardware-based security for remote access (such as a VPN) and provides secure wireless connections, as all the device protection in the world won't save you if sensitive data is transmitted in an insecure way

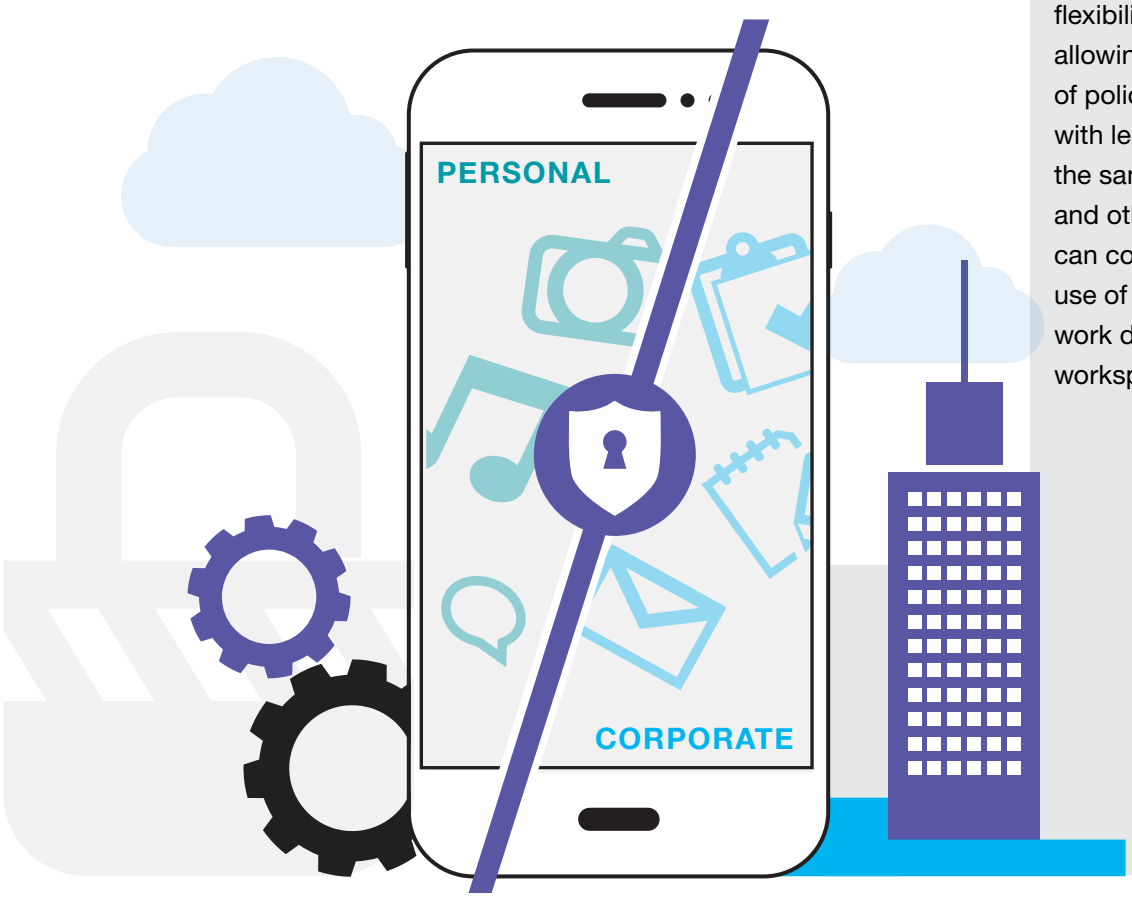


A Case for Multilayered Security

Samsung Knox, a security platform built in to the latest Galaxy smartphones and tablets, is a case in point for the value of multilayered security, making it an excellent fit for healthcare use cases. Knox protects the integrity of the entire device, from the hardware to the application layer. This multilevel approach to security includes tamper-evident fuses built into the device from the factory, combined with Trusted Boot, TrustZone based Integrity Measurement Architecture (TIMA), and Security Enhancements for Android providing real-time protections throughout the entire device life cycle. Knox received the most "strong" ratings of any mobile security platform in the Gartner report "Mobile Device Security: A Comparison of Platforms."

2. **Certificates and certifications:** Digital certificates form the basis for most security solutions, but if the certificates can be compromised, or if spoofed certificates can be installed, many of your other protections have suddenly evaporated. Therefore, it's critically important that your device provides a secure storage location for all security certificates. Additionally, the operating system is a key element in security, so be sure your OS is designed for and around security. Lastly, your applications should also support the required level of security, and potentially include features such as individual authentication (in addition to device authentication) and data encryption. The government has a number of certifications dealing with information security. Federal Information Processing Standard (FIPS) 140-2 is perhaps the best known of these certifications, at least in the U.S. Identifying a solution with FIPS 140-2 and/or other government certifications is a great start, since the government has done a lot of the initial work for you.
3. **Containerization solutions:** As mentioned earlier, in many scenarios, a personal environment will coexist with the corporate environment on a single device, regardless of whether the device is owned by the organization or the employee. Many employees will not want — or tolerate — the same high level of security in their personal environment that is demanded in the corporate environment. To solve this problem, you need a system that allows for the separation of personal and corporate space on the device, with separate rules of behavior for each. Since many corporate data breaches start with malware innocently installed by employees on their devices, it's critical that the device not allow any contamination from one environment to the other.

To learn more about Samsung Knox, visit samsung.com/knox



Separating Hospital and Personal Data

Containerization solutions like Samsung's Knox Workspace establish protected environments for healthcare applications and data. Designed for use in regulated industries like healthcare and government, Knox Workspace separates, encrypts and protects enterprise data from attackers. It provides flexibility and peace of mind for IT, allowing admins granular control of policies, and integrates deeply with leading MDM solutions. At the same time, physicians, nurses and other healthcare workers can continue to enjoy personal use of the device without risk to work data stored in the secure workspace.

Conclusion: Mature Approach to Healthcare Data Security

Mobile data security is not a simple matter, but it can be argued that the future of healthcare depends on it. The consequences of weak security when dealing with healthcare data are hugely significant. In light of the numerous data breaches over the past 18 months, every healthcare organization should be acutely aware of the risks and their responsibilities. With that in mind, organizations must be extremely diligent about the choices they make when implementing healthcare IT and mobility solutions, and the hardware platforms on which they run.

To find out more about Samsung's secure mobile solutions for healthcare organizations, please visit samsung.com/healthcare

Sources:

1 "Mobile Officially a Staple in the Doctor's Office," eMarketer, March 26, 2015.

2 "IDC Worldwide Quarterly Mobile Phone Tracker," December 2, 2015.

3 "Patient Adoption of mHealth," IMS Institute, 2015.

4 "Health App Use Among US Mobile Phone Owners: A National Survey," Journal of Medical Internet Research, Vol 3, No 4 (2015) Oct-Dec.

5 "Mobile health app revenue to grow tenfold by 2017, study predicts," Modern Healthcare, May 22, 2014.

6 White House webpage on the Precision Medicine Initiative, accessed June 2016.

7 White House blog on Precision Medicine Initiative and Data Security, dated May 26, 2016.

8 "Data Breaches In Healthcare Totaled Over 112 Million Records In 2015," Forbes Magazine, Dec 31, 2015.

9 "The Black Market For Stolen Health Care Data," National Public Radio (NPR), Feb 13, 2015.

10 "Most Cyber Attacks Occur From This Common Vulnerability," Forbes Magazine, March 10, 2015.

11 "Juniper Networks Mobile Threat Center Third Annual Mobile Threats Report: March 2012 through March 2013," Juniper Networks.

12 "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," Ponemon Institute, May 2016.

13 "OCR Should Strengthen Its Oversight of Covered Entities' Compliance With the HIPAA Privacy Standards," US Department of Health and Human Services, Office of the Inspector General, September 2015.

14 "OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities," US Department of Health and Human Services, Office of the Inspector General, September 2015.

15 "St. Joseph Health Settles Class Action Data Breach Lawsuit," Healthcare Informatics, March 2016.

A Mobile-Centric Security Assessment

For many healthcare IT departments, mobility is something that just "happened," rather than being strategically planned and implemented. The first step in moving to a more strategic approach to the use of mobile devices and apps is to conduct a comprehensive mobile security assessment. Samsung has partnered with Booz Allen Hamilton to create a mobile-centric security assessment model that helps organizations to effectively identify and address gaps, and understand the solutions available to effectively manage mobile devices.

For more information, visit: samsung.com/mobile-security-assessment

Learn more: samsung.com/healthcare | insights.samsung.com | 1-866-SAM4BIZ

Follow us: youtube.com/samsungbizusa | @SamsungHealth

linkedin.com/company/samsung-in-healthcare

SAMSUNG

WHP-HHP-HEALTHCARESECURITY-NOV16SW