July 2020

Secure Telehealth–End-Use Device Security, the Weakest Link

The COVID-19 pandemic is forcing a global shift to telework, impacting all industries and individuals. At the forefront of this shift is that of Telehealth. Actions being taken out of urgency, bring into sharp focus the realization that healthcare providers are poorly equipped to deliver telehealth while maintaining cybersecurity and data confidentiality. Security is being touted via cyber-secure cloud services using "HIPAA compliant" software applications. Yet, deploying these services and Apps on questionably secure remote devices is a recipe for disaster. The weakest links are the end-use mobile devices, where everything from laptops to smartphones are being deployed.

The false sense of cloud-based security provided to insurers, systems developers, and healthcare providers exposes HIPAA data to identity thieves and opens our entire health records infrastructure to malicious actors. The COVID-19 pandemic emergency cannot be used as an excuse of poor cybersecurity hygiene!

Data Privacy and Security is a Shared Responsibility.

Data Privacy and Security – A Shared Responsibility **Security is only as effective as the weakest element**				
Role	Responsibility	Critical Security Activities		
Cloud Host Provider	Security of the cloud	Compute / Server resources	Data storage and back-up	Networking & 3rd party services
Cloud Application Provider	Software as a Service security (SaaS) in the cloud	Role-based application authentication and privilege controls		
		Application firewalls, cloud interfaces and VPN interfaces		
		Client data encryption, integrity checks, and back-ups	Server file system and database configuration and encryption	Authentication, integrity and encryption of network traffic
Healthcare Provider	Security in the Application	Roles & Permissions configurations	User and Admin role assignments	User account administration
End-use Device (EuD) Provider / Manufacturer	Effective cybersecurity protections on the EuD	Operating System (OS) security, including timely patches & upgrades	App Store application security to prevent exploitation	Hardware security to prevent compromise of the OS and Applications
Customer / Patient	Proper use and maintenance of personal data and access credentials	Physical security of the EuD	Cyber Hygiene – timely updates, avoid risky emails and suspect Apps	Use of strong passwords and two factor authentication

Bottom Line Up Front**: Redwall Mobile®** security is the only end-device cybersecurity solution designed specifically to protect, separate, and control classified information on mobile devices. HIPAA/HITECH compliance requirements are no less stringent yet end use device security is largely reliant upon device operating system security, with its endless exploit-pay-patch cycles. *Why accept anything less that real security-delivered when financial futures and lives are at risk?*

Redwall Technologies is the sole provider of Redwall Mobile®—demonstrably the premiere mobile device security solution featuring Secure Persona® multi-user experience providing unparalleled separation between all data and apps of each user (or user role).

Redwall is Military Grade – Commercially Available:

- Shipping worldwide on multiple Motorola Solutions Inc. products, and featured on the LEX L11
- Redwall led MSI's recent successful National Security Agency, National Information Assurance Partnership (NIAP) certification for classified use of a mobile device (LEX L11)
- Redwall Mobile is fielded on other platforms to customers with the highest security requirements
- Redwall is actively seeking and engaging new mobile device partners to secure telework and telehealth devices (smartphones and tablets) against heightened threats and weakest link (end use device) vulnerabilities to enterprise health IT systems

Redwall Mobile® is the mobile device security solution proven to withstand intensive and extensive Government testing and rigorous use by military and first responders. It is based upon US Patents 9514300 and 9990505 and is ideally and intentionally suited to address the end-device security vulnerabilities being introduced by the rapid shift to telework and telehealth in response to COVID-19. Through its **Secure Persona®** solution, it solves the bring your own device and end user device security conflicts and enables one device to serve as many –enterprise, personal, patient, private or more!

Redwall Mobile Serves…

Mobile Device Providers – To equip remote and home care clinicians and practitioners for mobile work. Mobile device access may occur at patient locations, in office, and in hospital. Therefore, *the security of the mobile device is the first and most critical link in HIPAA/HITECH compliance*, data, and healthcare system security. A compromised mobile device can be used to compromise the entire system.

Healthcare Providers – Who are required to deliver services in increasingly difficult circumstances. Patient separation and isolation make monitoring and care delivery increasingly reliant upon mobile and telehealth solutions. These providers, and their IT staff are ill equipped and under resourced to address cyber-security risks introduced by the shift to telehealth and use of *vulnerable mobile devices*.

Healthcare Insurers – Who rely upon accurate and timely health-record and request for payment requests. These organizations bear the brunt of improper, incorrect, and fraudulent record-keeping. These providers, and their IT staff are ill equipped and under resourced to address cyber-security risks introduced by the shift to telehealth and use of vulnerable mobile devices.

Software Application, Cloud Platform, and Telehealth Providers – That are at the forefront of the shift to telework and telehealth. They play a vital role in enabling telework and the telehealth continuum of care, including securely linking patients to their providers and their electronic health records, and protecting those records in transit and at the host site. However, no software can be fully HIPAA compliant; it is up to the end user and the end use device security to ensure that they are using the platform in a HIPAA compliant manner. Simply stated, *these providers must rely upon the security of the end-use device to protect them, their client systems, and patient data.*

Redwall is prepared to eliminate the vital end-use device security weaknesses that, if unaddressed, will compromise enterprise and Healthcare IT systems. We are prepared to partner with mobile device, healthcare, cloud & health IT systems providers, and insurers to deploy mobile workforce and healthcare delivery solutions that will provide an exceptional remote experience, and a patient-centered continuum of care.

About Redwall

Our mission is to provide high-quality and highly effective cyber-security expertise, software engineering, and leading-edge technology to assist public sector agencies and private sector companies in preventing and responding to emerging threats against their mobile applications and connected infrastructure. We accomplish this by applying our technology to mobile devices and delivering capability through existing distribution channels to enable rapid adoption and sustainment while providing a distinct competitive advantage to our partners and device platform providers.

Contact:

John Rosenstengel
President and CEO
Redwall Technologies, LLC

John.Rosenstengel@redwall.us
937.477.0424 (cell phone)
937.956.6156 (work phone)
www.redwall.us