# Telehealth – Securing the Weakest Link

## Telehealth is Becoming the New Normal

The COVID-19 pandemic is forcing a global shift to telework, impacting all industries and individuals. Actions being taken out of urgency bring into sharp focus that healthcare providers are poorly equipped to deliver telemedicine while maintaining cybersecurity and data confidentiality. The weakest links are mobile devices, where everything from laptops to smartphones are being deployed. Having cyber-secure cloud services using "HIPAA compliant" software applications running on unprotected remote devices is a recipe for disaster. The false sense of security provided to insurers, systems developers and distributors, and healthcare providers exposes HIPAA data to identity thieves and opens our entire health records infrastructure to malicious actors. This emergency cannot be used as an excuse of poor cybersecurity hygiene!

## Redwall Mobile® Secures the End-Use Device

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. Redwall Mobile® is the mobile device security solution proven to withstand intensive and extensive Government testing and rigorous use by military and first responders. Why accept anything less that real security-delivered when financial futures and lives are at risk?

Redwall Mobile ® Security and Secure Persona®
Secure Persona™
Personal
Patient
Private
One device – many personas!

# The Ultimate in End-Use Device  Security

Redwall Mobile's® patented N-Persona Technology effectively turns one smartphone or tablet into as many device modes as desired, each with its own apps, data, settings, and security posture. Redwall Mobile® consists of modifications to the Linux kernel and Android operating system plus additional functionality. Redwall Mobile® is compatible with a wide variety of devices and technologies, which sets it apart from other software application-based solutions. Redwall Mobile provides features that even combinations of all competing device security technologies cannot match.

*Redwall Mobile® consumes minimal system resources and users do not know the device is hardened with military-grade protection.*

## Temporal Isolation in Addition to Cryptographic and Other Methods

Cryptographic and temporal isolation ensure there is no possibility of contamination across modes. It is as if the user is carrying separate devices within a single device.  Contrary to containerization where sandboxing or virtualization is employed, these methods cannot provide the level of isolation available in Redwall Mobile®.  Those containerized solutions still leave sensitive data in memory, making them highly vulnerable. Dedicated devices like the Blackphone are not the answer, requiring users to carry multiple devices for different roles or different levels of security. Redwall Mobile® consolidates all the features of a military-grade locked-down device with multiple personas in a single device. Our off-the-shelf devices are suitable for BYOD, reducing cost and complexity, all in a single device.

## Redwall Mobile® Technology:

- Has been commercially deployed domestically and internationally for more than five years
- Has blocked 100% of all zero-day attacks and malware for five years running
- Is completely configurable, from the number of modes to the availability of device resources
- Has also been deployed on IoT devices and is applicable to most connected devices