Mobile Security in Domiciliary Care

Access personal data securely from mobiles and tablets

trustd

THE PROBLEM

Confidential information is held on all devices - not just computers and laptops

It's not just medical records. It's any information that "relates to and identifies an individual". So this includes people's names, next of kin or family members, email addresses, physical addresses and dates of birth.

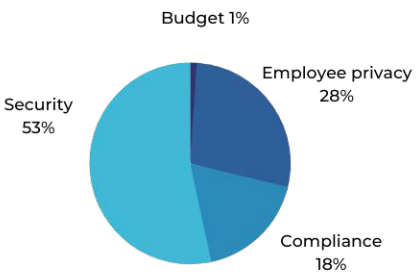
Your care staff are out and about, trying to give the best possible care to their patients. Sharing information is a critical part of primary care, but it's vital that it is done safely, securely and within the bounds of regulatory guidelines.

Caregivers aren't always technical wizards. So you need the simplest, most robust solution to ensure private data is protected, confidentiality is respected, and your organisation is compliant at all times.

> *People's personal records, including medical records, should be accurate and kept safe and confidential (outcome 21)*

CareQuality Commission

What concerns were your top blocker to implementing a BYOD strategy?



Traced poll of 191 IT Governance professionals May 2021

THE SOLUTION

A robust MTD to guard against data loss

Unlike other solutions, Trustd combines AI-powered mobile protection technologies, straightforward user guidance and accessible pricing to protect customers against mobile malware, phishing and data theft on Android and iOS devices.

It can support your Cyber Essentials and GCloud applications, compliance with GDPR guidelines, and enforce your duty of confidentiality. Enable your Zero-Trust mobile strategy by restricting access to company data from untrusted devices, whether they're managed by an MDM/MAM or unmanaged.

HOW DOES DATA BECOME COMPROMISED?

Network threats (Android & iOS)
- Man-in-the-Middle attacks
- Phishing
- Malicious scripts
- Malicious proxies
- Unsecured WiFi
- Weak WiFi security

Device threats (Android & iOS)
- OS exploits
- Vulnerable configuration

App threats (Android)
- Malware apps
- Known and unknown threats
- Screen recording
- Leaky apps
- Camera/Microphone access
- App permission abuse

The Trustd app on employee devices protects against all these threats.

SECURITY MADE SIMPLE

A simple administrative console anyone can use.

- See which devices are enrolled and protected
- Comply with data protection regulations
- High-level views ensure employee privacy
- Identify threats and remediate straight away
- Standalone MTD or integrate with your MDM

KEY FEATURES IN SOLUTION

- **WiFi scanner** alerts when an employee connects to a compromised WiFi network
- **Web checker** protects against phishing attacks and malicious websites
- **OS update alerts** identify potentially vulnerable devices
- **App analysis** to identify malicious apps and permissions abuse (Android)
- **Integrates with your EMM** or straight into Microsoft Azure AD for zero-trust
- **Privacy at its core** so employee activity on their phone stays private

Start a free trial.

We've made set-up and enrolment as simple as you could hope for, so to get started in under 2 minutes, go to traced.app/control and set up a free trial.