CommandHub
securing sensitive information

CommandHub Use Case

Healthcare

How to Secure Collaboration on Confidential Patient Data

USE CASE: Healthcare

How to Secure Collaboration on Confidential Patient Data

Your Situation

You are the IT Manager, Operations Manager or other Senior Executive for a large healthcare organisation, which provides medical services via private hospitals and nursing homes. You might also offer at-home services for senior citizens through regular visits by community nurses.

The individuals involved include nursing staff, doctors, physiotherapists, psychologists, case workers and care coordinators. Some of these are direct employees and others are external. They operate as an extended team, collaborating on patient data, medical histories, home care plans, family histories and other highly confidential data in order to provide the required services.

Your Challenge

Tablets are popular with mobile health care workers and physicians, providing access to vital patient data from the hospital, clinic or patient's home. These devices can also take photographs, which is vital for recording incidents as well as tracking patient recovery in facilities and their own homes.

With so many healthcare individuals accessing and updating patient files, your challenge is to secure this confidential information at all times. Equally, you need to enable authorised access and use, without so complicating the process that users are tempted to seek risky work-arounds.

Your Vulnerability

Protecting patient data is of the utmost importance, not just to comply with regulations and avoid embarrassing leaks, but to maintain an open, trusting environment among health care workers, patients and their families.

Use of mobile devices exposes confidential patient data to heightened risk because:

- Encryption is compromised because the key is stored on the device
- The cache leaves sections of recently-viewed material accessible
- In the event of theft, remote wiping is ineffective as soon as mobile and WiFi access are disabled.

Your Options

If securing the sharing of sensitive content among your health care teams is critical, there are four main options:

1. **Do Nothing.**
   This may appeal if you've had no breaches to date or none has been reported. Even if you feel that your current rules and processes are working, this would unlikely be a realistic option, given the sensitivity of patient data.

2. **Choose an Enterprise File Sharing System.**
   These systems make file-sharing easy and provide some file security but are not designed for collaboration. You'll need to add third party tools which could add cost and complexity and open security gaps. This would be your choice if lowering rather than eliminating risk to patient data is enough.

3. **Choose Enterprise Collaboration Tools.**
   These widely-used tools were designed to facilitate collaboration with security added later. You may find that specified security levels apply to the environment not the tools, and that user configurations require a great deal of IT help. This would be your choice if your patient data is not critical, mobile device use is not widespread and your IT resources are not stretched.

4. **Choose an End-to-End Secure Collaboration Platform.**
   This approach, in use for over a decade, creates ultra-secure content compartments to which access is restricted on a 'need to know' basis. It extends protection beyond who accesses your content to how it is used and where it is stored, including on mobile devices. This would be your choice if you need complete end-to-end protection of patient data, and your risk profile demands a proven solution.

How CommandHub secures your sensitive collaborations

Military Grade Architecture

CommandHub was designed from the ground up for secure collaboration, based on the Military Principle of multiple layered servers. This provides multiple levels of document encryption and infrastructure protection.

The CommandHub solution is IRAP certified to the Australian Signals Directorate (February 2020) ISM PROTECTED standard. All data is wholly hosted and managed in Australia under the Sovereign Cloud Principles for Critical Infrastructure.

Patented End-to-End Protection

Providing the highest level of server security is the minimum; CommandHub also provides content protection in transit and in use. With patented HubVault technology, health care teams can securely access and use patient data on mobile devices, via a multi-encrypted tunnel that replaces vulnerable browsing. HubVault also secures content stored on mobile devices, using further encryption and a non-recoverable key, rendering them 'uncrackable' if they're mislaid.

'Need-To-Know' Compartmentation

CommandHub applies the Intelligence Community principle of compartmentation, restricting user access to a 'need to know' basis. This means that even personnel with high seniority will only be granted access to specific compartments if they 'need to know' the contents for their roles.

Logical Business Controls

CommandHub makes collaboration easy for healthcare teams while ensuring that your organisation's business processes are followed.

You can set controls for who can see, edit or save a file, who may move it and to where, how approvals and rejections apply, the exact sequence of these steps as well as version control, watermarking, file-locking and more.

Ease of Setup, Use & Control

CommandHub was designed for setup and use without IT skills. After little training, your administrators will be able to arrange patient data logically for your health collaborators and apply controls to protect it. As services or patients transition, administrators can make the changes themselves. For collaborators, the intuitive interface makes collaboration easy without IT support.

Tailored to Your Exact Needs

With over 500 configuration settings, CommandHub can be fully tailored to how your organisation operates. By simply turning on or off rules for files, access, use, formats and settings at any level, CommandHub ensures that your patient data is fully protected, without impeding how your health care teams work.

Proven In Situations Like Yours

CommandHub has been protecting sensitive content in the most demanding situations for over ten years, in Health, Justice & Law Enforcement, other Government, Defence Contracting, Banking, Insurance and Telecommunications, and for Executive Committees elsewhere. Ask us about our case studies.