

Case Study

SafeSuite Lite ensures protection, control, and visibility of patient data emailed outside the hospital network.



Situation

A hospital coordinator sends a patient's Discharge Summary, which includes sensitive health information, to an external home health agency for continued care. This routine task, typically done via email for convenience and speed, ensures a seamless transition of care.

Challenge

- Contains HIPAA-regulated data
- Leaving hospital's security perimeter
- Sending to party with unknown security
- Recipient can forward, download, print
- No control or visibility once sent
- Emails can be misaddressed or hacked

Where Traditional Defenses Fall Short

Standard Encryption

Once downloaded, the file is unprotected and uncontrolled.

Data Loss Prevention (DLP)

DLP offers no protection once the file leaves the network.

Digital Rights Management (DRM)

Poor recipient experience; limited policies, control, and no visibility.

While encryption, DLP, and DRM offer important pieces of the puzzle, none provide persistent, adaptive, user-friendly protection once the sensitive file is sent.

Solution

With SafeSuite Lite, the hospital coordinator easily and confidently shares the sensitive files directly from email, without disruption or compromise.

Embedded Protection

Advanced encryption and policies stay with the file beyond your network.

Granular Access Policies

Policies define who, when, where, and how access is granted and can be modified any time.

Frictionless Access

Recipients don't need any new software, downloads, or accounts.

Instant Revocation

Access can be revoked entirely, even after the file is shared and downloaded.

Full Visibility

Maintain full visibility of all access attempts with detailed forensics.