Security Guardian Use Case: Health Sector

Customer

Major UK National Health Service Trust responsible for delivering a full range of health services from education and preventative medicine, day treatment centres, routine admissions and surgery and full Accident & Emergency (A&E) facilities.

The trust has over 15000 staff, 7 major hospitals, 11 community hospitals and works with 93 General Practice surgeries.

Challenge

With increasing pressure on budgets and increasing costs the trust needed to identify significant costs savings whilst maintaining care and standards across their entire portfolio of service delivery obligations.

The Trust required a way of providing access to medical records without the need to supply mobile devices or expensive BYOD security infrastructure

Mandatory requirements:

Robust hardware that can be carried by on-site employees.
Secure storage for patient medical information
Data only available in authorised areas.
No user intervention required
RFID as secure access to authorised areas
Secure VPN communication when required

Solution

Following detailed discussions about the range of mandatory requirements, ExactTrak supplied Security Guardian units that include an advanced Geofencing function which addressed one of the core required functions for the securing of data. This involved having a product that would only become active once it with was located within an authorised area such as health centre or hospital. Security Guardian was approved for use by all community nurses and outbound medical staff. Security Guardian includes integrated GPS, GSM, RFID and rechargeable battery

In operation:

At the start of each day the Security Guardian units are loaded with the appropriate patient records and relevant information for each patient. By default the data is turned Off and access can only be achieved when Security Guardian arrives at an authorised location. If additional clinical information is required whilst at a centre Security Guardian provides a secure VPN connection to a central database.

The embedded RFID chip provides access to authorised areas. In cases of loss or theft the ability to remotely destroy the device and its memory store helps ensure that data loss penalties are avoided.

The verifiable audit train that is maintained by the management console is available as proof of the robust mobile data security policy and can be produced to confirm that at all times the sensitive data has been secure or destroyed.