Social Care Data and Cyber Security Programme Case Study

Elizabeth Finn Homes

Controlling and protecting personal and sensitive data in care homes using computer-style terminals called 'thin client devices'

As we use more technology in care services, both to support care delivery and to improve digital connectivity with partner organisations, it is vital that people's information is kept secure, and that the systems we use are reliable. As part of the National Cyber Security Programme, the Local Government Association, Care Provider Alliance and Department of Health and Social Care commissioned the Institute of Public Care (IPC) at Oxford Brookes University to undertake a research programme to support the adult social care provider sector to manage the business risks associated with data and cyber security.

The research took place from October 2018 until March 2019 in three local authority areas: North Yorkshire, Central Bedfordshire and the Royal Borough of Greenwich. A representative sample of seventy care providers operating in these areas took part, including Elizabeth Finn Homes, which operates a portfolio of 10 care homes across England, catering for around 500 people who require supported living through residential or nursing care. The care homes use digital records for client data and care plans to ensure secure, efficient access to information.

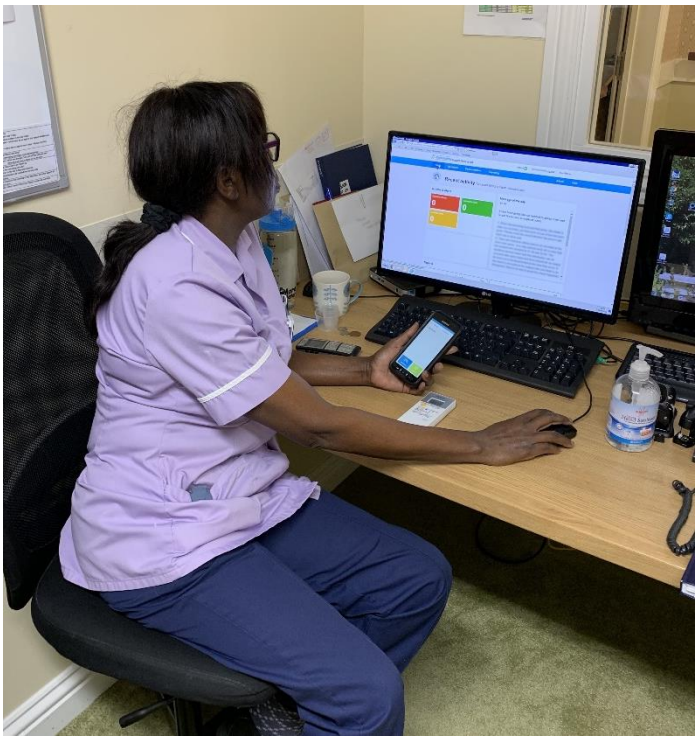
Elizabeth Finn Homes is a wholly-owned subsidiary of a charity called Turn2us whose mission is to combat poverty in the UK. Any surplus generated by the care homes helps fund the charity. The IT for both organisations is shared and managed from within the charity. This includes managing three million searches per year as part of the charity's benefits calculator service. The need for security and reliability around data access systems is clearly vital.

The Director of IT for Turn2us and Elizabeth Finn Homes commented, "*For Elizabeth Finn Homes, the aim was to create a centralised system that was efficient, low maintenance, secure and fit for purpose."*

Elizabeth Finn Homes installed terminals, called 'thin client devices', in each of their care homes. To an everyday user, these terminals look like computers with a Windows 7 operating system and login. However, unlike a computer, the terminals

have no hard drive or storage capacity, instead the system just displays images of a normal Windows-configured desktop, without the local functionality. There is no information stored on the terminal. Instead, all the information is accessed remotely via a secure internet connection to the computer server held at Elizabeth Finn Homes' head office in London. Care home staff access the programmes and information they need using a staff log in with a user-name and password.

Each of the 10 care homes operated by Elizabeth Finn Homes has between 10 and 15 terminals. This typically includes one or two on each care station, and additional terminals for the Clinical Care Manager, Administrator and General Manager. These terminals are all connected to a dedicated internet line which exists only to run the 'business side' of the care home.



These terminals, or 'thin client devices', are used by staff to access personal and sensitive care data and to update care plans, client records and medication data, which includes eMAR (the Electronic Medication Administration Record). In addition to client data, staff personnel data is accessed via the terminals. This includes scheduling and rotas, pay details and annual leave information.

The system needs a good broadband connection to operate effectively and the availability of this would be something to consider in scoping out the feasibility of such a scheme. Elizabeth Finn Homes secured a fibre optic leased line from BT Broadband and this ensured not just transfer speed but 'low latency', with the result that when a staff member uses the computer mouse to access information via the terminal screen, there is no delay in transmission; for example, a half second time delay between mouse movement and on-screen action would lead to a very poor user experience! All data being carried on Elizabeth Finn Homes' network provision is via BT Broadband using a VPN – a Virtual Private Network – which makes the internet connection more secure. The VPN means all communications are encrypted and secured at source so the staff member using the terminal never has to consider security when sensitive data is being transferred, as their communications always travel over an encrypted line.

Whilst electronic measures secure the system, there are also policies around logins, passwords and staff access. Staff training at induction includes sight of the IT and data confidentiality policies and staff signatures are required to show these have been read and understood. Key management staff use a personal login to access their terminals, whilst junior staff have a shared terminal login which gives joint

access to shared logistical information. A secondary level personal login is required for junior staff to access or edit Care Records and eMAR, as appropriate. Staff currently change their passwords every six months, although this policy is now under review, as latest research shows regular password changes mean staff are more likely to jot down the details as a memory aid, adding to the security risk. The Central IT team review the list of active user accounts at each home on a quarterly basis, checking that staff leavers have been taken off the system.

In addition to the dedicated 'business' internet connection which connects the terminals, each of the care homes have an additional and physically separate internet connection which provides connectivity for the public Wi-Fi for residents and guests, which is also used to access staff training resources. In fact, perhaps the only disadvantage of running a 'thin client device' system such as this, might be its inability to run media effectively – such as videos or podcasts – as the terminal display screens and systems aren't designed for multi-media usage. At Elizabeth Finn Homes there is limited use of these tools, and staff development and training videos are provided on a separate laptop which connects to the 'public' Wi-Fi.

In order to negate any potential risks of having a single point of failure, meaning the central system breaks down or experiences 'downtime', Elizabeth Finn Homes has prepared a protocol for loss of service, which varies dependent on the length of outage. This protocol includes keeping paper records for a very temporary loss of service, printing out records by head office and distributing to the care homes as required or in an emergency, re-purposing the public WiFi broadband and or the use of a mobile device 'hotspot' utilising 3G or 4G cellular mobile phone network' and sharing that connection with nearby laptops and devices.

Over the 10 years this 'thin client system' has been operating, modified and improved there have been no incidents of data breach or concerning outages.

Key benefits and outcomes

- **Sensitive data is stored on servers** – effectively large computers – held at head office, which are controlled, locked down securely and maintained by the professional IT team who can employ best practice at all times. There is no sensitive data held on computers or laptops in the homes.
- **Reduced costs of ownership** - a terminal and screen is less costly than a computer, and furthermore, the maintenance, support, set up and training costs are reduced by having central access and control.
- **Licensing costs are reduced** through using this centralised system, with Elizabeth Finn Homes needing to license for devices to access the servers and the software on them, rather than multiple Windows computers.
- **Centrally managed operating systems** means updating is managed by the IT department and only approved software is permitted. This helps reduce the risk of introducing malware or a computer virus because a program has to be approved before it can run. The IT team re-build the servers each month to refresh the service and ensure consistent and efficient access.
- **Central backups of data** are held offsite. Care records and eMAR are hosted and managed in the cloud.

- **Reduction in travel time for IT staff** who can maintain systems from head office in London, rather than travelling to 10 geographically remote homes. The system also features tools to support and help staff by remotely taking control of the screen with a desktop sharing tool.
- **Disabled for USB storage devices** - data can't be copied across from the terminals to a USB storage device.
- **A high level of security** is offered by the business and public internet connections being physically separate, although in time a fibre optic line could be installed to increase broadband efficiency and this could be electronically separated and secured.
- **VPN-secured laptops for remote workers** mean that staff accessing sensitive data away from the care home can connect to the central system via a secure VPN system and using a two factor authentication system. Two factor authentication means you sign into the system with your username and password and then enter a code that is sent via text (SMS) to your phone, using a phone provided by Elizabeth Finn Homes. It means that both devices need to be in someone's possession in order to login.

Overview of investment

- **Six substantial computer servers that act as 'remote desktops'** - around 30-35 terminals are logged in to each server at any one time.
- **Up to 200 terminals** made up of a 'thin client device', wide-screen, mouse and keyboard (terminals are used by both the charity and care homes).
- **A fibre optic leased line in** HQ in London provides high speed internet to transfer data down the line to the care homes from head office.
- **A high-quality broadband connection** to each home.
- **Staff training** in use of devices and IT policies.

The ongoing journey

The IT team for both Turn2us and the homes is small: just two experienced IT professionals and a database expert. Their director says, *"The system has huge advantages in terms of the investment costs, maintenance and ease of support but it also has the benefits of high availability and low downtime, and comes with a wealth of robust security features built into the set up – which means staff never need to consider the security of their communication. As with all systems we are continually reviewing our set up, our security and our policies to stay in line with best practice."*