Data and Cyber Security Research in the Technology Enabled Care sector

Executive Summary

July 2019

Final draft – 22.07.2019

Executive Summary

The Technology Enabled Care (TEC) sector involves the provision of services such as telecare (long distance monitoring of people to support them to live independently at home) and telehealth which provides arrangements for people to manage short and long-term conditions.

It is estimated that 1.1 million people in England are currently supported through the provision of TEC. High service availability is critical for TEC services since it is the first point of contact should someone have a fall or experience other deterioration. These are often life-saving services. It is therefore essential that arrangements are in place to prevent cyber or data security incidents occurring since, in the event of failure or malfunction risks could include death or serious injury to clients.

Currently the majority of TEC connections are over traditional analogue telephone lines with notifications sent from devices in the home (such as a pendant alarm) through to the Alarm Response Centres (ARCs). Upon receipt of a notification ARCs will then ensure that a person in need of support receives an appropriate response. However, OpenReach has stated that by 2025 these traditional lines will be switched off although there is already evidence of the switchover beginning to take place which is beginning to impact on the reliability of alarm services.

This digital switchover will have a sizeable impact on the TEC sector with the vast majority of devices (and indeed non-TEC devices such as landline phones and alarms) needing to be upgraded or decommissioned. This presents a risk but also an opportunity to move towards digital forms of connectivity using full internet or cellular connectivity rather than traditional lines to communicate with ARCs.

It is in this context that the Local Government Association, Care Provider Alliance and Department of Health and Social Care commissioned the TEC Services Association (TSA) to carry out research with a range of ARCs across England. The discovery was aimed at:

1). understanding the extent to which Alarm Response Centres have begun to embrace the switch to digital,

2). highlighting the data and cyber security risks for TEC services and

3). considering where further support may be needed to mitigate the risks to this sector.

What is the picture for Alarm Response Centres?

The research carried out by TSA involved on-site engagement with 21 ARCs from a range of council, housing association and privately delivered centres. These ranged from centres providing services to 2,500 clients to 180,000 clients. The research size accounted for 13% of the total number of ARCs in England (158 in total).

The majority of ARCs are delivered in house by councils (72%, of which the majority of these are district councils), by housing associations (19%) and then by the private sector (8%) and community interest companies (1%).

86% of services provided by ARCs are purchased by councils, housing associations or CCGs and 14% by private individuals (those not receiving health or local authority funded services). 7 in 10 of the ARCs provide in-person responder services which enables them to respond after someone has suffered a non-injury related fall. In more serious cases, emergency services will be alerted to respond.

The research found that Alarm Response Centres fell into two categories:

- **Type one organisations** that primarily use analogue systems and have limited exposure to new technologies. These organisations typically employ traditional (analogue) technologies and have very little experience of internet or cellular connected devices. They remain dependent on third party software suppliers for the main operational platform used by call handlers to respond to alerts from the home.

- **Type two organisations** mostly use digital or (as in many cases) a combination of analogue and digital systems. They are organisations who are embracing the switch to digital and the new technologies. Typically these organisations have strong business continuity arrangements, staff are given data and cyber training and have IT skilled staff on-site 24 hours. However, the greater use of digital technology puts them at greater risk compared to type one organisations given the use of ‘always on’ devices and greater use of analytical use of data from such devices.

The research found that the split between these personas was relatively even with 57% of ARCs falling into type one and 43% into type two personas.

There was also some correlation between the size of organisation and whether organisations fell into type one or type two personas. 76% of TEC services were part of larger organisations and therefore in many cases benefit from services provided by the larger organisation (e.g. within a housing association or council) although of course this meant that such technology is not always supported by specialist IT support in life critical alarm systems. In some cases where ARCs are part of larger organisations they will often operate quite autonomously from the organisation to which they belong.

Despite 43% of organisations falling into the type two persona typically the number adopting fully digital services remains low. Across all organisations the research found that only 14% of TEC service providers have adopted internet protocol (IP) connected devices at scale and adapted systems, infrastructure and processes indicating that significant work is required in this area over the next few years. This figure is low given the move to digital by 2025.

The research found that multiple IT systems are used throughout the course of TEC delivery. Four software suppliers dominate the UK market for ARC monitoring with Jontek and Tunstall platforms account for 89% of UK monitoring platforms. However, whilst information sharing was often undertaken through encryption there were very few examples of system interoperability. Opportunities exist in information sharing at three levels:

1). Between external organisations (e.g. Local Authority) and ARCs

2). Within ARCs themselves (for example between customer relationship manager (CRM) and monitoring systems)

3). Between ARCs (for example when someone moves provider)

Given that TEC services play a critical role in supporting integrated and personalised care, the need for interoperability within TEC services will increase and there is an opportunity to strengthen this area of work.

As part of the service provision ARCs service collect and store personal and confidential health and care information on individuals they support such as medical issues and medications alongside demographic information, next of kin details and keysafe information. It is therefore critical that such information is kept safe and secure.

Data and cyber security risks

The research identified variations in the awareness and planning for data and cyber security risks across the sector.

A key theme of the research identified the need to strengthen approaches to systems and processes and for more robust network security and technology management practice.

Despite observations, the level of threat for traditional (analogue) systems was found to be low-to-medium although there is, as yet, no commonly adopted standard for data and cyber security in the TEC sector.

However, the shift to digital presents significant increases in risk if this shift is not well managed. This was identified as the overarching risk in the research. In particular there are three areas of cyber and data security risk with associated with the digital switchover:

1). **Risk at a device level** – either from devices which are fully internet enabled (e.g. hackers accessing the device directly) or from cellular devices where risks relate to SIM card misuse (e.g. family or friends removing the SIM card and using it for other purposes)

2). **Risk at a software level** – from software which monitors the devices and is usually managed by 3rd parties

3). **Risk at an ARC level** – from issues in relation to cyber or data incidents occurring within the Alarm Response Centres themselves

The research identified opportunities to learn from countries such as Scotland and Sweden who are further advanced in their preparedness for the switchover.

The focus of the work was on assessing risk in Alarm Response Centres given this is felt to be the area where should incidents occur it would have the biggest impact. Further work will also be needed in relation to individual devices (such as supporting organisations to ensure SIM cards are locked to devices) as well as directly with IT suppliers to ensure steps have been taken to minimise the risks of a data or cyber security incident.

Across each of the 21 ARCs involved in the research, the discovery looked at areas of risk categorisation based on the National Cyber Security Guidance. Overall, there was a relatively even split between organisations rated as red (32%), amber (37%) and green (31%) although unsurprisingly those type one organisations that have lower levels of digital maturity will have a higher risk rating.

Overall risk rating	Type one organisations	Type two organisations	All organisations
Red	30%	2%	32%
Amber	20%	17%	37%
Green	7%	24%	31%
Total	**57%**	**43%**	**100%**

Across each of these areas the highest risk areas were in systems and processes (52% of organisations had an overall red risk rating), network security (43% of organisations had an overall red risk rating) and technology management (43% of organisations had an overall red risk rating).

Given the current use of analogue rather than digital connectivity for many devices the threats are currently reduced but this will shift as ARCs increasingly adopt cellular or digital forms of connectivity.

Specifically these risk areas were:

1). Systems and processes – in particular the need to support smaller ARCs with patching of devices across the estate which will become increasingly important with the shift to digital;

2). Network security – in particular the need to support commissioners and ARCs with effective control and security at an individual device level e.g. effective password management across the estate;

3). Technology Management – in particular the need to support ARCs with the transition to new service models associated with the digital switchover e.g. the move to cloud based services;

Whilst overall the ARCs demonstrated that they had put in place steps to reduce the impact of a cyber or data security incident very few had fully taken the step towards embracing digital TEC services. This is for a number of reasons including lack of clarity around the impact of the switchover on existing devices as well as funding challenges associated with investing in brand new kit. Further support will be needed in this area to ensure the switch to digital does not heighten the security risk.

Awareness of national support

Only 33% of study participants were aware of the Cyber Essentials Toolkit with a similar (but different cohort) number (29%) aware of the Data Security and Protection Toolkit (DSPT). Both of these tools have been designed for organisations to ensure that robust data and cyber security arrangements are in place. The DSPT was seen as less relevant to TEC services given the use of the TSA Quality Standards Framework although is being increasingly used by the adult social care provider sector.

Alarm Response Centres highlighted opportunities to enhance their cyber and data security approach by inclusion of cyber and data security elements into standards such as the Quality Standards Framework. However, it is worth noting that whilst the Quality Standards Framework is adopted by many suppliers this is not exhaustive and therefore any approach to raising of standards across the TEC sector needs to take into account the mixed sector approach.

Recommendations

For national bodies

1. TSA and other appropriate bodies to upgrade their quality and standards frameworks to incorporate aspects of data and cyber security, particularly in light of the digital switchover. These standards should be drawn from the National Cyber Security Centre, NHS Digital (Data Security and Protection Toolkit) and other related sources.

2. Work should be undertaken by NHS Digital and TSA (and other appropriate bodies) to look at the interface between the Data Security and Protection Toolkit and quality frameworks to reduce duplication in submission.

3. Department of Health and Social Care / NHSX to work with NHS Digital, TSA and other associated bodies to ensure all Alarm Response Centres are meeting data and cyber security standards.

4. Department of Health and Social Care / NHSX to commission specific support to the TEC sector regarding the digital switchover (for both service providers and commissioners) and in particular preparedness in the area of data and cyber security. Support should focus on the following areas:

    a. Guidance and support to reduce the risk at an individual TEC device level;
    b. Liaising directly with suppliers of TEC platforms to perform due diligence and share the findings with all TEC customers (ARCs and commissioners);
    c. Guidance and support to reduce the risk for ARCs.

5. Further work to be undertaken between TSA and Department of Health and Social Care / NHSX to learn from the Scottish approach to the digital switchover (particularly regarding data and cyber security) to be taken into account for the completion of recommendation 4.

6. Further work to be undertaken by the TEC sector (coordinated by TSA) to explore opportunities to strengthen interoperability and information sharing including the development of information standards for ARC to ARC sharing of information and ARC to business (e.g. council) sharing of information.

7. Guidance on the use of health (medical data) in TEC services. This should include improving the understanding of the extent to which medical information (e.g. medications, medical conditions) are used within TEC services and the extent to which this can be used (e.g. medication data and reminders used by monitoring services).

For service providers (including in-house services)

8. Alarm Response Centres (ARCs) to be encouraged to complete the Data Security and Protection Toolkit (DSPT) if they are handling information related to the health or care of an individual (e.g. medical information).

For commissioners

9. When contracting for telecare services, to include requirements for data and cyber security in contracts and service specifications, with particular reference to the issues identified by this review.