2020

Data and Cyber Security Guidance for TEC Services

Local Government Association

TSA™

The voice of technology enabled care

Digital Social Care

Data and Cyber Security Guidance for TEC Services

Acknowledgements

We are grateful for the contributions from the Technology Enabled Care (TEC) sector (Alarm Response Centres (ARCs), ARC software suppliers, local authority commissioners) and national bodies, which enabled TSA to gather views and intelligence for this guidance document.

Contents

1 Aims and objectives

This guidance is intended for public sector commissioners, Alarm Receiving Centre (ARC) operational managers and staff, technology suppliers and stakeholders in the Technology Enabled Care (TEC) industry. It has been commissioned by the Local Government Association on behalf of the Care Provider Alliance and NHSX and informed by ARCs, commissioners, and TEC software suppliers.

The material provided here is intended to highlight the particular needs of the TEC sector as they relate to data and cyber security, and should be viewed as assistive information alongside the guidance that is available through:

- National Cyber Security Centre – provides a range of cyber security guidance and resources including the government backed scheme Cyber Essentials
- Digital Social Care - a dedicated online space for care providers containing tailored data and cyber security advice and guidance
- NHS Digital – the NHS Digital Data Security and Protection Toolkit is an online tool enabling organisations which process care and health information to self-assess their data security approaches

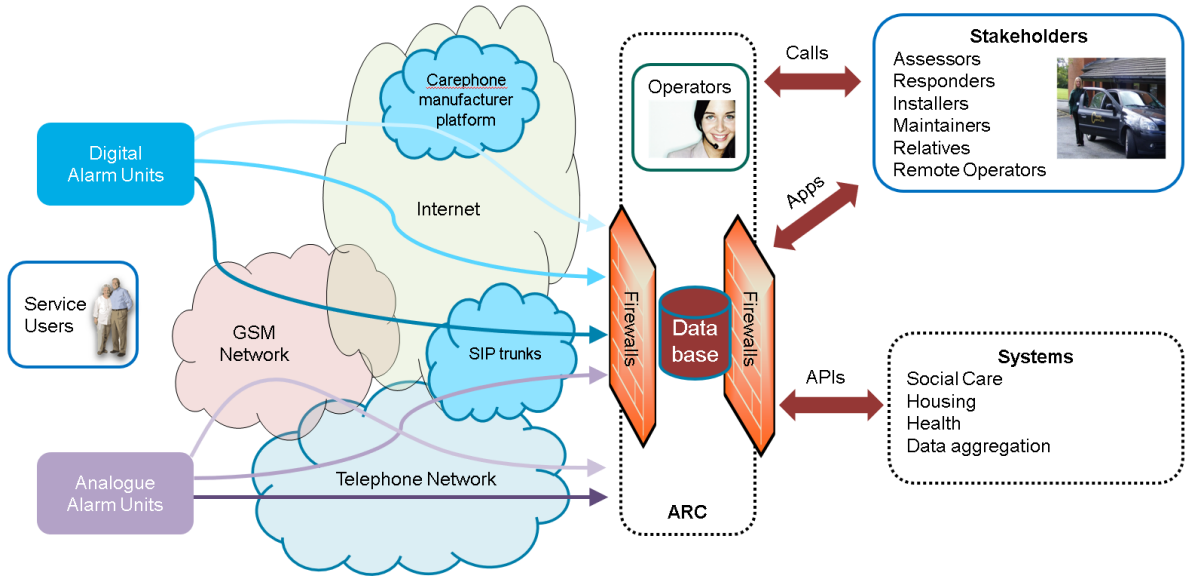
This document is intended to support key stakeholders in protection of TEC assets from data and cyber security threats, and it makes recommendations for those commissioning, purchasing, and operating all elements of Technology Enabled Care. It is a follow up piece of work on the 2019/20 discovery project undertaken by TSA to identify the key data and cyber security risks in the TEC sector. It is based on experiences since the implementation of the Care Act and is not formal guidance and should not be applied as such. It should be used to have conversations about how the issues raised can be dealt with locally. It does not constitute legal advice and should not be relied upon in that capacity. Independent legal advice should always be sought.

It is intended that this guidance information could be embedded and maintained in any quality frameworks that relate specifically to the TEC sector, (e.g. TSA Quality Standards Framework).

2 How data flows into and out of an Alarm Receiving Centre

It is important to understand how data is used and stored in a technology-enabled care setting if we are to examine risks and protective measures. The diagram below gives an indication of how data is transferred, from a variety of different routes from the individual to the Alarm Receiving Centre that is monitoring that individual's alarm:

ARC Communications and data flows



The above diagram shows how alarm data is passed to the ARC, who take appropriate action with the relevant stakeholders in the process (e.g. ambulance services for suspected injury or fire services for fire or smoke alarm).

In practice, the 'information models' for individual TEC services may differ, as the services offered to users will vary, and any information being exchanged with other users or partner organisations will have an impact, and these need to be considered carefully.

Therefore, an important early step is to produce a clear picture of how information is being captured and used by an organisation, so that the risks and impacts of any data and cyber security threats becoming an incident can be examined and then reduced.

More detailed diagrams representing both the process flow of information through the differing roles/resources and the technical flow through the connected technology architecture can be found in appendix 5.

3 Specific cyber security guidance for stakeholders

The following section sets out in more detail the specific guidance for key aspects of the alarm monitoring process.

The 2019/20 discovery project identified the following key areas where there are risks of cyber attack and data breach within the TEC sector:

1. **Risk at a device level** – such risks may relate for example to TEC devices which are fully internet enabled (e.g. hackers accessing the device directly) or to 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** – software applications are invariably used to manage the main functions of an Alarm Response Centre (ARC), including monitoring of

alarm devices. This software is usually provided and sometimes managed remotely by 3rd parties. The associated data may employ on-site storage at the ARC, or back-up locations, or through 3rd party support, and may employ cloud storage. Software applications often interface to other systems, thereby presenting points of entry and potential vulnerability.

3. **Risk at an ARC level** – from issues in relation to cyber or data incidents occurring within the Alarm Response Centres themselves. These incidents might relate for example to human failures, or failures of process, which expose the ARC to data and cyber security risks.

Risks and guidance focused on equipment and devices can be found primarily in sections 3.1-3.2 below; risks and guidance relating to ARC monitoring software and the function of the ARC itself can be found in sections 3.3-3.5.

TEC commissioners and data controllers should follow NCSC guidance on managing the supply chain from a cyber security perspective. All the components of the social care alarm industry detailed above come under the supply chain and it is ultimately the data controller's responsibility to ensure these suppliers comply with the requirements for protection of personal data.

There are a number of principles that could be followed by TEC commissioners and data controllers to ensure best practice across the organisations that they are partnering with, to deliver good outcomes using social care alarms. These principles are summarised in Appendix 1.

3.1 TEC supplier engagement

There are a number of questions that commissioners could ask of their suppliers to better understand their data and cyber security measures and arrangements.

The range of technology-enabled solutions available to care services is ever-increasing, particularly driven by the need for new and effective services, innovation and interoperability from commissioners, the emergence of procurement options, and the increasing consumer awareness and demand for technology that is more aligned to the devices used in our everyday lives, such as mobile apps, smart sensors, smart speakers and voice assistants.

The following considerations may assist ARCs and commissioners in supporting data and cyber security within TEC services:

- a clear end-to-end service delivery model, including identification of any other health or care services that are involved
- definition of the intended purpose of the services provided, including objectives they are looking to achieve for both those they support and their overall services
- a clear picture of how information is captured, used, and protected
- the ability to communicate and enforce any underlying requirements in relation to suppliers of enabling services, equipment, or other technology.

It is important to promote a message of collaboration and partnership with suppliers of TEC solutions – an efficient and effective service will be driven by outcomes, rather than being technology-led. ARCs and commissioners are encouraged to seek supplier relationships that address the needs of data and cyber security, working in partnership to mitigate risks, rather than a purely transactional relationship.

Technology or enabling service suppliers could be asked to complete an Information Governance questionnaire as part of the 'informed dialogue', and before their solutions are adopted within TEC services. This encourages consistency across the TEC sector, benefitting ARCs and commissioners by ensuring that solution suppliers provide comparable information on their infrastructure, data security and robustness of their operations, and benefitting the solution suppliers by being able to share consistent information with potential customers they interact with.

Please refer to Appendix 2 for a set of questions which could be considered for inclusion in any initial engagement with potential suppliers. Please note that these should be combined with any specific questions / requirements that may arise from each ARC service.

3.1.1 TEC device manufacturers

Historically the TEC device marketplace was made up of a small amount of large 'tried and trusted' TEC suppliers but recent years has seen the introduction of new entrants to the market, particularly as TEC equipment has become less niche and more generic and accessible to the general public.

Commissioners should look to ensure the following information is known and understood about each device before proceeding with a procurement decision:

• **Digital roadmap** – TEC services typically rely on the exchange of voice and data of telecommunications networks, and these are switching from public telephone connections and point-to-point communication to networks which exchange IP (internet protocol) packets of data. Therefore, the testing of any TEC devices on "all-IP" telecommunications networks is recommended to ensure that these devices will work in the medium to long term.
• **Data collection and transmission –** open but secure protocols for transmission are preferred to enable the integration of information from multiple sources. This means that organisations can share appropriate data automatically in a safe way protecting against unauthorised access to that data.
• **Data storage locations** – guidance is that data should be stored within the European Economic Area
• **Business continuity** – if the transmission of information from and to the device passes through the device manufacturer itself, then it is recommended that stakeholders ensure the manufacturer has a robust disaster recovery plan in place
• **Interoperability** – free at the point of access and open standards are recommended
• **Commercial viability** – relevant financial checks should be carried out as part of the standard procurement process; new entrants should not be discouraged but risk of supplier failure should be mitigated

• **Accreditations** – while ISO and TEC industry accreditations are not mandatory, TEC device manufacturers should be encouraged to seek independent auditing of their policies and practices
• **Security** – TEC device manufacturers should ensure all steps have been taken to protect their devices from unauthorised access, particularly with regards to GPS location devices where there have been well-publicised instances of unauthorised access

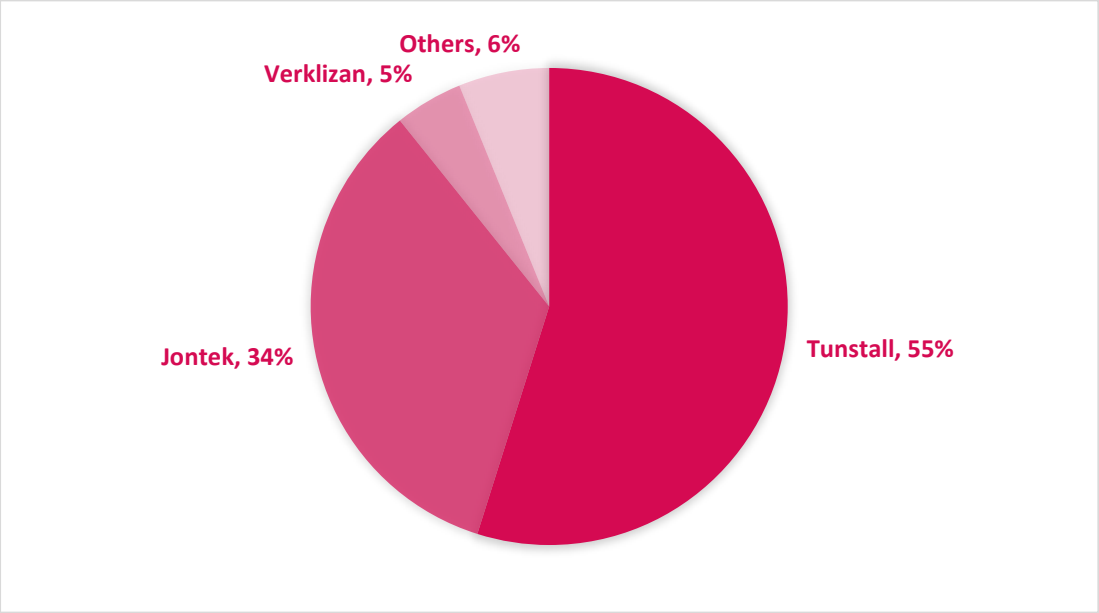
It can be expected that suppliers of stand-alone devices will not be able to address all aspects of the questionnaire presented in Appendix 2. In this respect, TEC service providers or commissioners should ensure that best endeavours are taken (for example, seeking input and guidance from both Information Technology and Information Governance departments to help provide assurance to the procurement process).

We recommend that a 'system authority' is identified for any TEC service (this could be the most technically capable resource available within the organisation or an independent expert), so that overarching challenges can be addressed, including:

- partial system responsibility for performance
- information ownership
- end to end testing
- interoperability
- change management
- standards compliance

3.1.2 ARC software suppliers

The UK marketplace for social care alarm monitoring is made up of a small number of vendors broken down as follows (data collated from ARC feedback by TSA in Autumn 2019):



From a cyber security perspective, the ARC suppliers need to have clear policies and

procedures in place which should be tested regularly with key partners, especially key plans covering business continuity, disaster recovery and incident response.

There are varying methods of deployment of ARC hardware and software. Historically, ARCs have been a closed environment that could only be accessed by specific computer terminals on the commissioner's site with no connection to the commissioner's corporate network.

More recently, cloud-based infrastructure has enabled ARC servers to be hosted off the commissioner's premises and through a range of devices (i.e. laptops and mobile phones). These new deployment methods, whilst clearly beneficial to all stakeholders, brings with it increased cyber security risk.

From a cyber security perspective, TEC commissioners / data controllers could consider the following areas as part of the formal procurement of an Alarm Receiving Centre solution:

Functional requirements • Access to the hardware and software is secure • The user interface is browser-based to support multiple access methods • Password reset should be a self-service administrative function • Passwords should comply with NCSC guidance • Robust security permissions should be configurable to role and individual level
Data requirements • Clarify ownership of data • Confirm termination conditions for data and transfer of data upon termination • All data to reside within the EEA at all times • Data retention policy of the ARC should match that of the controller
Business continuity requirements • ARC should clearly state end to end options for continued delivery of service • There should be robust Disaster Recovery testing policies in place
ARC infrastructure requirements • ARCs should provide diagram of interlinking components for cloud or enterprise solution • Data controller should be clear on automatic interface requirements e.g. to social care, housing, or health • There should be separate ARC environments for production and development which enables a clear testing ground for future development • End to end encryption of data under transfer should be mandatory • Where cloud software is being deployed, the 14 principles of cloud computing should be adhered to

4 Other considerations

There are several aspects of the commissioning and delivery of TEC services which need to be considered alongside the specific cyber security guidance.

4.1 Analogue to digital shift

TEC systems are broadening from social alarms to include other assistive technologies and applications, such as social inclusion, activity monitoring, self-managed care, telehealth and social media support, using a variety of digitally-connected and increasingly intelligent devices around the person, their home and their mobile environment. These changes to TEC applications will require that any measures adopted in relation to data and cyber security will need to be re-examined.

Telecommunications networks are also changing, migrating from analogue connections to digital networks that see only packets of internet protocol (IP) data. This creates opportunities in terms of faster connections, richer datasets and 'always-on' connectivity, but also threats such as lower resilience to power failure. Service providers should be aware of the changes so that services can be managed accordingly. More information about the switch to digital can be found on the TSA website including the recently published "10 Facts about the Analogue to Digital Shift" (see Appendix 3).

4.2 Technology management

Technology management is an important aspect of data and cyber security risk management. This is usually considered in the context of maintaining software and operating systems in a known and current state, so that defences to bugs and cyber threats are kept up to date. With the introduction of digital TEC, we can foresee that challenges to technology management will extend into the homes and lives of vulnerable users, given that devices increasingly depend on their own embedded software and cyber defences. Whilst service providers and commissioners cannot always influence the types of devices that are being purchased privately by individuals to support their everyday lives, they can sign post to guidance for how individuals and families can increase their level of cyber protection (e.g. https://www.ncsc.gov.uk/section/information-for/individuals-families)

From a digital device perspective, the telecoms industry's plan to migrate its entire analogue network to digital by December 2025 has meant organisations have taken significant decisions already – the main decision being whether to continue to purchase analogue equipment based on guarantees from those manufacturers that the equipment will continue to work in a digital environment with the relevant adaptors or to move to digital equipment working initially in an analogue environment or a hybrid environment of analogue and digital infrastructure.

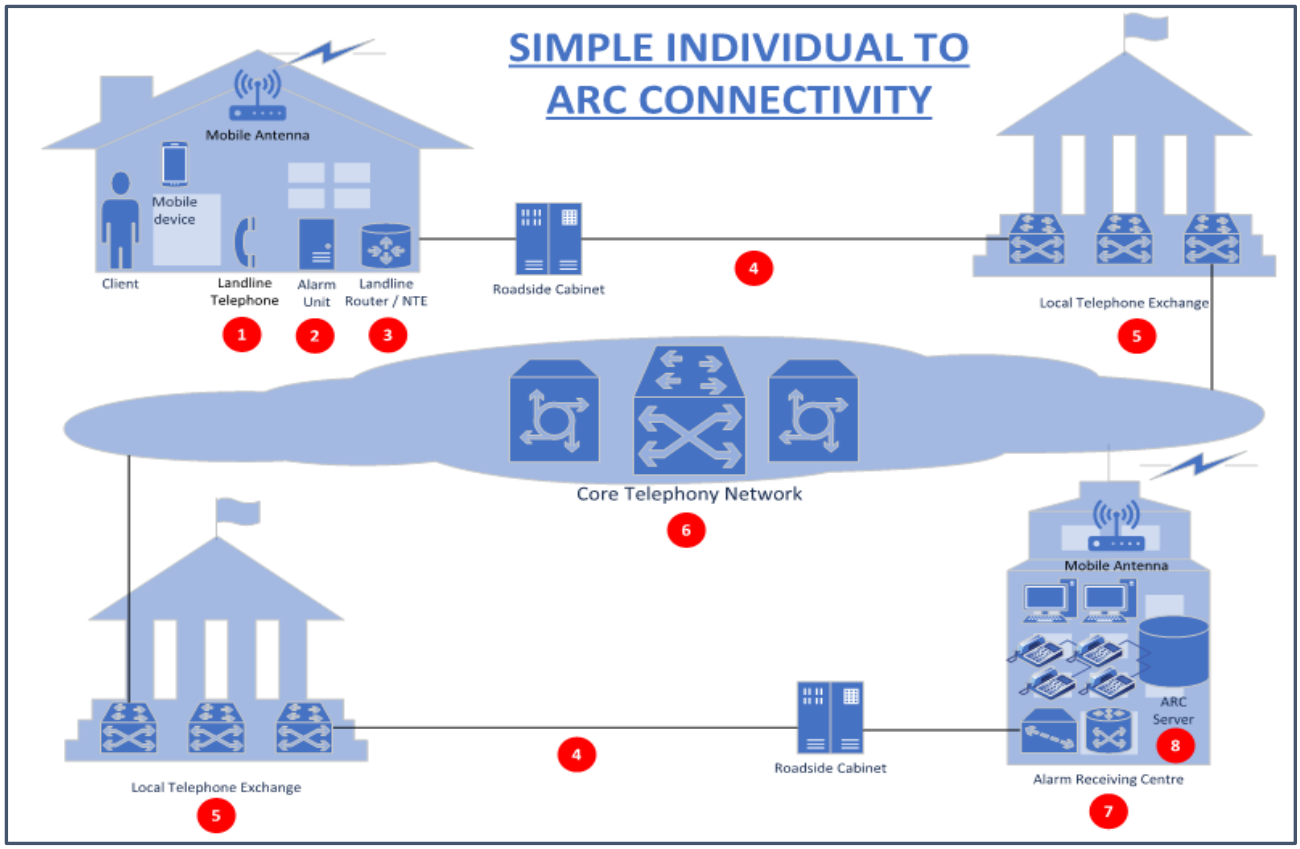
To support an organisation's planning for usage of analogue and digital solutions, and the potential cyber risks involved, guidance on the strengths and weaknesses of each approach is set out in Appendix 4.

4.3 Business continuity

Research completed in 2019, across a range of Alarm Receiving Centres in England, found a range of solutions in place to ensure alarm calls could still be monitored in the event of a

disruption to service.

When considering a business continuity solution, stakeholders in the monitoring of vulnerable service users should understand the end-to-end technology that underpins the service and the steps that should be taken to mitigate any potential failures. The diagram below illustrates a simple end-to-end telephone network (reality is more complex), to give an understanding of where single points of failure exist and steps to ensure business continuity:



1. The **Landline Telephone** is normally funded by the individual as part of their personal utilities and the Alarm Unit is connected using the landline router or wall socket (Network Terminating Equipment) a. The landline is normally within the individual's control, but the ARC should record details of the landline telephony provider (e.g. BT, Virgin, etc.) so they can be notified that the property contains an Alarm Unit that is life critical.
2. The **Alarm Unit** is provided by the TEC Commissioner or Alarm Receiving Centre. a. The unit is normally configured to connect to one of either analogue landline, digital landline or mobile network but some alarm units have the capability to connect to more than one communications network which enables greater network resilience – note that a connection to a mobile network will incur monthly recurring charges from that network

b. To comply with the Quality Standards Framework for Technology Enabled Care, all alarm units should contain at least 24 hours of battery back up in the event of a mains power failure.
c. Digital alarm units will also provide the added benefit of a regular 'heartbeat' so that the ARC will be notified when a unit is offline.
d. Alarm units are configured to dial the ARC number in the event of an alarm trigger – consideration should be given to programming at least two ARC numbers into the unit in the event of a failure of the primary number (the secondary number should be deployed on a separate comms network – e.g. primary BT, secondary Virgin)

3. The **Landline Router or Network Terminating Equipment (wall socket)** connects the landline telephone and the alarm unit to the external communications network. If the landline is analogue then it is likely that the alarm unit will connect directly to the NTE (wall socket) supplied by the communications provider (e.g. BT / Virgin etc…) whereas if the landline has been converted to digital then a landline router will provide the connectivity to external network.
    a. If the alarm unit is plugged into the landline router then a battery backup solution that encompasses the router should be considered – a 24 hour minimum is recommended in the TEC Quality Standards Framework.
    b. If the alarm unit is connected directly into an analogue NTE (wall socket) then the alarm unit will still be able to make a call to the ARC under a mains power failure situation due to the power provided from the local telephone exchange which is capable of powering the NTE.
4. The '**local loop'** is the external connectivity between the individual and the ARC and their appropriate telephone exchanges. The loop contains the roadside cabinet that often connects copper and optical fibre strands of the network within specific geographic locations. ARCs should consider diverse network routing that mitigates against a failure in the external cable routing or cabinet by providing separate network routes from the local telephone exchange to the ARC.
5. The **Local Telephone Exchange** houses the communications infrastructure for a geographic region. To mitigate against a failure in a local exchange, an ARC can request dual parented exchanges so the alarm calls can be routed through a separate telephone exchange should one exchange fail.
6. The **UK Core Telephony Network** is a high-speed mesh that covers the country linking Local Telephone Exchanges together allowing both calls and internet traffic to travel around the UK at appropriate speeds with appropriate levels of quality. Some telephony providers use Least Cost Routing across the core network which reduces the wholesale cost of the call but can affect call quality. ARCs should register the telephone numbers dialled by the Alarm Units with comms providers via the TSA email address (allip@tsa-voice.org.uk) so that those dialled numbers are added to a protected list of numbers where Least Cost Routing will not apply.
7. The **Alarm Receiving Centre itself** contains the people and the relevant technology to manage incoming and outgoing communication with individuals via their Alarm Units. At least the various scenarios listed below and how these might be mitigated against for business continuity should be

considered (e.g. failover to another ARC, ability for employees to access data and telephony remotely, etc.) a. Access restriction to ARC building b. Loss of ARC building power c. Loss of communications network to ARC building d. Illness to ARC staff
8. The **ARC Server** contains the data relevant to the alarm service as well as the means of accessing that data and can be housed in the ARC building or in a separate secure location (sometimes referred to as 'the cloud'). ARCs should be linked to at least two servers in geographically separate locations, that replicate data and are connected to the ARC via different network routes so at least one server will be operational in many disaster scenarios.

4.4 Workforce development

It is recommended that organisations and their staff incorporate general good practice guidance around cyber security into business practices and induction plans.

Two recommended guidance sources are:

1. Digital Social Care – Cyber Security overview – containing several sections, in particular 'train your staff to be cyber aware' and cyber security resources, aiming to support staff to be aware of cyber threats in both their professional roles and their own lives
2. The Institute of Public Care (IPC) have led on cyber security projects focusing on the care sector, with the latest product from this work being guidance on 'safe use of technology in adult social care services'. Section 3 of the guidance – 'how to support providers with data and cyber security' contains a section (3.1) on signposting with links to a range of useful resources to support organisations in general to raise awareness among the workforce

4.5 Data storage and processing

There are a number of sources of guidance with regards to data protection in general. It is incumbent on all parties that are collecting, handling, storing, processing or sharing TEC data that they understand their roles and responsibilities within those processes especially given the likelihood that TEC data will contain information about a living individual.

As a standard at the point of a commissioned contract ending, where a new TEC service provider and ARC will be delivering the service going forward, it is recommended that it be a requirement of the incumbent service provider to transfer existing data held on the live alarm connections to facilitate a smooth transition to the new TEC service provider – it is recommended that a standard data transfer protocol and process is adopted, with the data presented in an interoperable format (PDF format is not acceptable) and transferred in a secure method such as FTP transfer.

The General Data Protection Regulation (GDPR) defines the legal basis for those data protection roles and responsibilities:

- The Data Controller determines the purpose for the data processing and in most cases, from a TEC perspective, the Local Authority will be the Data Controller as it will commission an organisation or service to work with that data on its behalf
- The Data Processor collects, handles, stores, processes and / or shares the data appropriately and this role within the TEC Sector is normally taken on by organisations such as Alarm Receiving Centres or device manufacturers
- It is also incumbent upon Data Controllers and Processors that this data should not be transferred or stored outside of the European Economic Area (The EU plus Iceland, Liechtenstein, and Norway)

As well as the legal framework set out within GDPR, there will also be local and regional guidance which those making procurement decisions about TEC services should understand – for example the completion of a Data Protection Impact Assessment (DPIA) is not a legal requirement but is set out in Local Authority policies and procedures in order to assess risk and to ensure that the processing of data is limited to data that is necessary for the requirement.

For further guidance, the UK's independent authority set up to uphold information rights in the public interest is the Information Commissioner's Office (ICO) and a link to their organisational data protection guidance is https://ico.org.uk/for-organisations/

Appendix 1: Summary of TEC supply chain principles (taken from NCSC supply chain security guidance)

1. Understand what data should be protected and why a. The likelihood of TEC supplier contract requiring the processing of sensitive data is high and the suppliers should understand and recognise this
2. Understand the TEC suppliers' security measures and the risk in the supply chain a. What building access / controls exist to prevent unauthorised personnel gaining physical access to supplier locations b. What controls are in place to ensure the suppliers communications and IT network access are restricted to authorised users only c. What steps have suppliers taken to mitigate security risks (e.g. assessment of employee risk, training on common cyber-attacks)
3. Communicate minimum security requirements / expectations to suppliers & sub-contractors a. Balance requirements with level of risk and cyber maturity of suppliers rather than forcing a one-size-fits-all approach b. Ensure contract termination and transfer clauses for data protection are included c. Set expectations for the training and awareness of supply chain staff in areas such as the Centre for the Protection of National Infrastructure (CPNI) security awareness campaigns
4. Build assurance activities into supply contract a. Establish Key Performance Indicators and build in regular security performance reporting for main suppliers b. Build the 'right to audit' into all contracts as well as acting immediately with any key security concerns flagged c. Consider additional requirements in the contract such as Cyber Essentials Plus, Data Security & Protection Toolkit (DSPT) entry level or Quality Standards Framework (QSF) certification
5. Build trust and continuous improvement within the supply chain a. Recognise that security requirements and guidance evolve, and expectations will adjust during the duration of the contract

Appendix 2: Suggested Data and Cyber Security Questions for TEC suppliers

Quality Assurance	Describe the quality assurance standards that your organisation operates to in the context of supplying technology or services to the care sector. Can you identify those aspects of quality assurance and your associated business processes which relate to information security?
Personally Identifiable Data	Describe the nature of the data that is used in your services or technology (how it is captured, operated upon, reported, stored, or transmitted by the TEC solution). Can you describe how consent for the use of data is managed? Can you present an information model that identifies the use of Personally Identifiable Information? Do you capture any information that would be classified as relating to the health of users, and if so, what measures are taken to ensure this is accurate and current? Example: current medications. Please ensure that associated business systems (such as scheduling, finance, and invoicing) are considered. Please include all aspects of personal data e.g. voice recordings.
Anonymisation and Pseudonymisation	Which aspects of the technology solution employ anonymised or pseudonymised information? How will you ensure that pseudonymised data cannot be matched with an individual user? Can you describe how consent for the use of data is managed?
	Example: How will installation / fault management / repairs of devices be handled to avoid matching data with users?
Past experience with the protection of user data within care services	Describe your scale and experience of managing information in a care or TEC service context? What challenges did you face, and how were these overcome? Have you been involved in any 'reportable incidents'?
How and where is data processed?	Does your organisation host or operate technology solutions on behalf of care or TEC services? Does your organisation store any personally identifiable information relating to the services you support? Where data is stored, is it encrypted? In which country and where are your application servers and any data stores based? Will data be transferred to, or accessed from, any countries outside the EEA?
Data and Cyber Security Principles	Can you describe your technology solution in terms of key components, other organisations, or systems that you interface with, any points of external access, and the main security principles that are applied to the protection of information? Do you have any relevant data protection impact assessment? Examples: How are authentication and access control measures applied to any external users, such as installation or service engineers? How is secure data transfer achieved between organisations? Do users and their families or carers access your information?

	What measures do you apply and what principles do you recommend in ensuring that TEC services meet their business continuity needs, with particular attention to secure and maintained data access?
	What policies and interfaces do you apply in terms of open interoperability of systems with other organisations?
Access	Who, within your organisation, will be authorised to access personally – identifiable or pseudonymised data, and for what reasons? Will access to the data be granted to any other organisations and how will this be protected? (e.g. sub-contractors or partners). Is user access to the recorded information restricted by default without prior authorisation?
Security Measures	Describe security measures which are used to prevent unauthorised access, accidental loss, or destruction of data: • During transmission • On your server
	Describe your approach to technology management, and how the status of technology components (e.g. operating systems, software applications) is kept up to date, and hence more resilient to cyber threats.
	What is your approach to regular reviews or testing of system security? Examples: Are your systems subjected to penetration testing? Do you apply proactive monitoring to identify unusual user behaviour?
Accuracy and integrity of data	Describe measures used to ensure that the data transferred to or employed by the Alarm Receiving Centre is timely, complete, accurate and secure.
	Would your technology platform retain any records after termination of services to users or after termination of a supply contract? If so, please explain why, for how long this would be considered necessary, and describe the process for deleting these records afterwards.
	How will you support the import and export of information at the set-up and termination of any supply agreement, so that the continuity of care services is assured, and that information security is preserved?
Information Governance	Do you have an information governance structure in place? Describe the structure briefly, including details of roles and personnel responsible for overseeing information security and data protection governance matters? What are their qualifications, expertise, and experience?
Managing risks	How do you ensure an appropriate balance between the need to share information to deliver optimal care outcomes, and the need to protect people against the abuse or misuse of their personal information? Please provide details of your processes for preventing, identifying, reporting, and managing information risks.
	Advise how data protection breaches or data security breach incidents of any kind are managed, including reporting loss of

	personal data as soon as reasonably practicable & notifying the relevant commissioning and regulatory organisations.
People, Awareness and Skills	How do you train and refresh your staff on information security, data protection and any associated governance standards and business processes?
	How do you ensure that access to systems and information is linked to appropriate roles and skills?
	What audit trails are available to monitor who accesses any relevant systems, equipment and data used to provide the services in order to ensure that processes are being followed correctly and that no information security or data protection breach has occurred?
	Describe your vetting and background checks processes carried out on the reliability of your staff, including employees, contractors, temporary workers. This should include both on recruitment and during their employment.
	Will there be a particular team working on this contract for the Commissioning organisation? Please provide brief details where appropriate of any applicable training or qualifications of key team members/ workers.

Appendix 3: 10 Facts about the Analogue to Digital Switch – TSA

1.	**As early as 2023, it will not be possible to buy an analogue phone line from BT**. Instead, BT will move its customers to a digital, Internet Protocol (IP) network, in readiness for the shut-down of all its traditional telephone lines.
2.	**In 2025 the traditional, Public Switched Telephone Network (PSTN) will be switched-off** and replaced with a digital 'all-IP' network. Voice calls and data (including telecare alarm calls) will no longer be sent via traditional point-to-point connections. Instead, they will be sent as 'data packets' over digital networks.
3.	**In 2025, all Integrated Services Digital Network (ISDN) lines will be switched off.** Many telecare services still use ISDN to feed alarm data, via multiple phone lines, into their monitoring centres. They will need to find alternative solutions.
4.	**With some digital migration already underway, analogue telecare alarm services are reporting a rise in the number of failed alarm call attempts**. One service provider has reported a failure rate of 11.5% (and rising) for the first alarm attempt.
5.	**Telecare alarms will fail due to loss of power to routers.** This is not an issue for alarms on the old phone networks - when power fails, these alarms have 24-hr battery back-up and phone lines still work. But when analogue alarms run on digital networks, they will rely on routers, plugged in at home, which will stop working during or shortly after a power cut. This also means that 999 calls will not be possible from fixed-line phones when power is lost. Telecoms providers have responded differently to this critical issue, but their proposals are limited. - BT have confirmed that their new router will come with one hour of battery back-up. - Virgin Media's router has no back-up at all and 'vulnerable clients' will be provided with a separate device that allows 999 and 112 calls only. These proposals unfortunately go against industry standards (EN50134) and best practice guidance, which all require 24-hour operation of telecare alarms in the event of a local power failure. Service providers will need to make risk assessments where systems are rendered non-compliant with standards and take any necessary mitigating actions.
6.	**Communications providers and Ofcom all recommend a shift to digital and away from traditional analogue devices.** This is because analogue devices, including alarms, send data as audible voice tones over the PSTN network. When they are connected via a digital network this 'voiceband' data could potentially be corrupted or lost. This has implications for the reliability and safety of for example analogue telecare systems. Other countries have already encountered this problem; Sweden launched a national digital upgrade programme after failed telecare calls were widely reported and a 76-year-old man died after his analogue alarm was unable to connect via the digital network. In fact, more than 95% of Swedish digital alarm installations now use mobile network connections.
7.	**Mobile networks may be essential to future UK alarm connection, however, Vodafone will switch off 3G in the next 'two to three years'.** The head of Vodafone's UK networks, Andrea Dona confirmed this in July 2019. 2G switch-off may also happen before the mid-2020s. It is vital that we guide telecare alarm services to

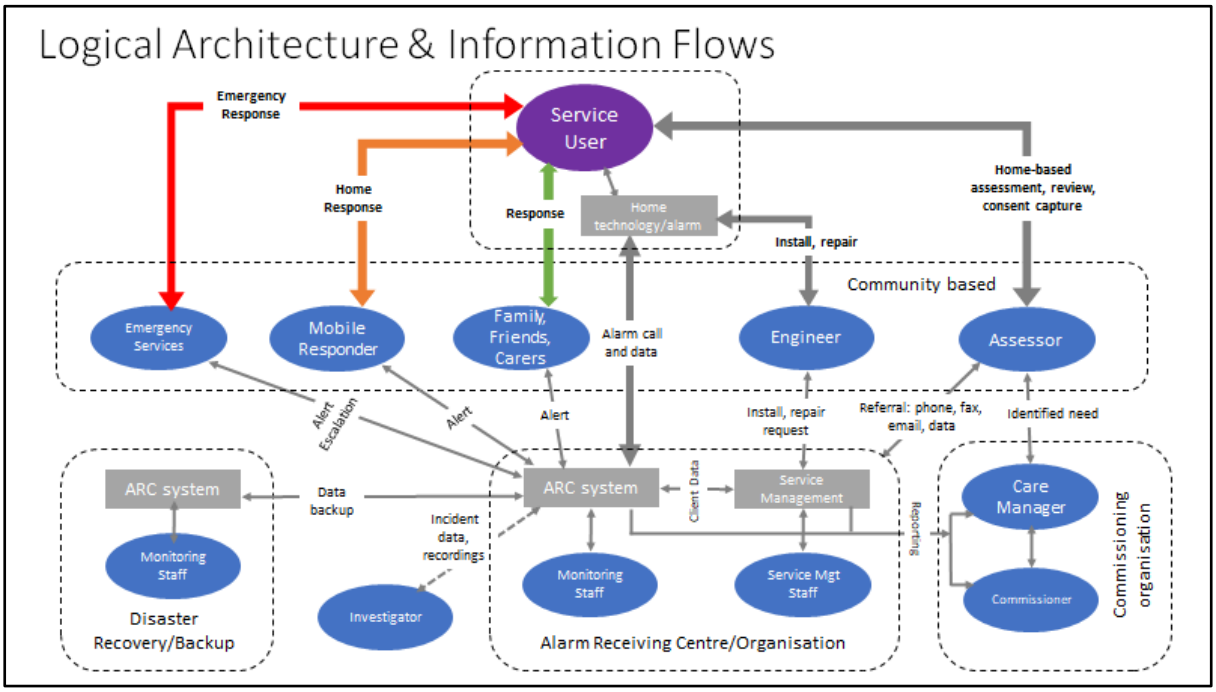
	the right mobile network options, as reduced coverage and eventual switch off will impact the quality and safety of these systems.
8.	**Awareness of the challenges posed by the digital shift varies hugely across the TEC sector.** TSA's research shows that digital maturity amongst telecare service providers differs enormously, as does their awareness of the digital shift. A large proportion of services providing telecare to vulnerable people have not even begun to upgrade their analogue equipment.
9.	**After a telecoms upgrade, communications providers are not committing to the re-installation and testing of telecare alarms.** Once they fit a connection, router and adapter device, engineers will only be permitted to check a new phone line connection is up and running– they won't necessarily test telecare alarms to make sure they work on the new digital network.
10.	**BT and Virgin Media currently use adaptors to connect analogue phones and telecare alarms to routers, but they have not yet guaranteed that these plug-in devices will be available in the long-term.** So, in the future, existing telecare alarms may not work over the new digital networks, or users may have to pay for an Analogue Telephone Adaptor (ATA). This would have cost implications for telecare service providers and vulnerable customers.

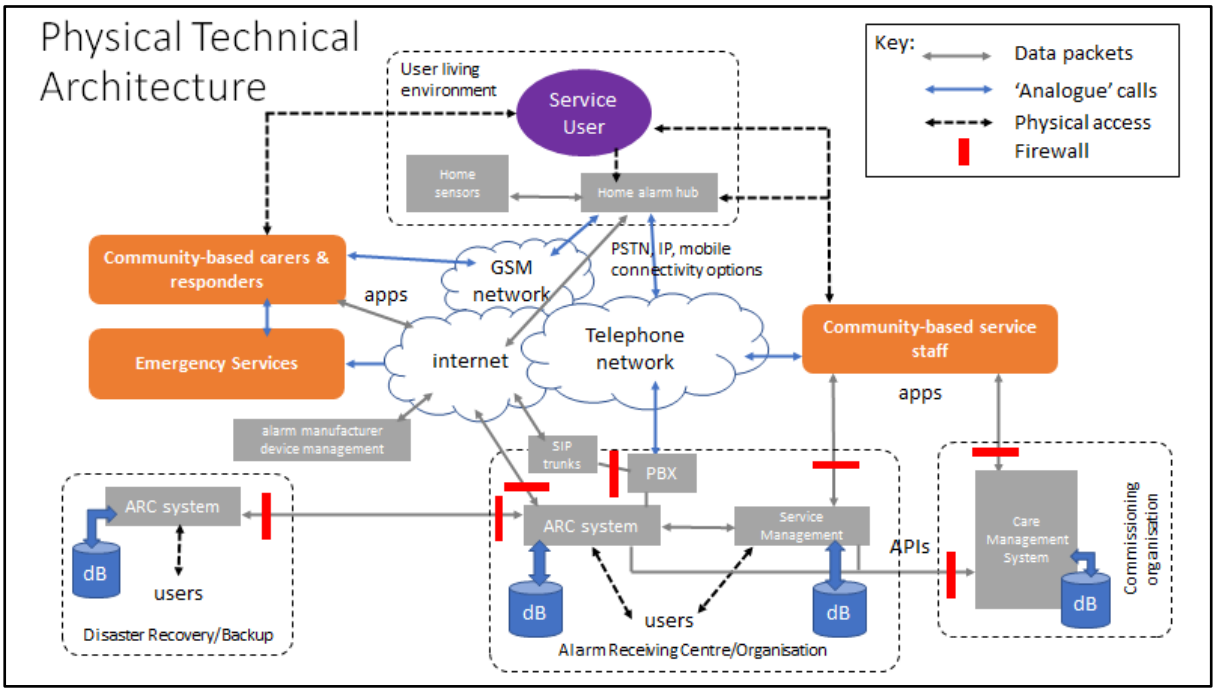
Appendix 4: SWOT Analysis of Digital Migration Options

	Strengths	Weaknesses	Opportunities	Threats
Continue to purchase analogue landline equipment only in the short and medium term	Allows further time to assess the marketplace with regards to a digital purchasing decision Lower short-term cost	Analogue equipment call failure rates will increase but it is not known at this stage to what extent Analogue landline equipment will run in shorter supply as manufacturers move to digital Not resilient to power failure, or standards compliant on IP networks		Should call failure rates rise above acceptable levels, it will be a more challenging task to replace analogue equipment in a shorter timeframe Liabilities associated with procurement and operation of non-standards compliant technology
Purchase digital landline equipment for new installations only, maintaining the installed analogue landline equipment base	Enables full value to be gained from the existing analogue equipment Provides a solution for those clients that have moved to digital landlines	Managing a mix of analogue and digital landline equipment for some ARCs requires a change in central site telephony Two-tier internal processes for managing both analogue and digital landline equipment can be challenging Additional monthly recurring cost if SIM used as a backup in case of digital landline failure Poses difficult challenges in	The digital landline equipment can provide a richer experience both in terms of capturing additional monitoring data as well as remote support and maintenance	As the digital landline equipment portfolio is still developing, early adopters of the first wave of digital landline equipment may find more advanced second and subsequent waves of equipment Digital landline equipment will fail in a mains power outage without adequate power and network backup

		terms of firewall protection over broadband		
Change all existing analogue equipment to digital in advance of December 2025	Increased capital investment required to bring forward digital changeover	Digital landline devices not fully tested on increasingly hybrid analogue/digital infrastructure or fully digital infrastructure Additional monthly recurring cost if SIM used as a backup in case of digital landline failure Poses difficult challenges in terms of firewall protection over broadband	The digital landline equipment can provide a richer experience both in terms of capturing additional monitoring data as well as remote support and maintenance	Digital landline equipment will fail in a mains power outage without adequate power and network backup
Move away from landline equipment to mobile network equipment	Removes the risks associated with the analogue to digital landline migration	Additional monthly recurring cost for SIM card usage UK network coverage is not 100%, particularly in rural areas Individual properties architecture can affect mobile network coverage		UK mobile networks are phasing out 3G networks in favour of 4G and 5G by 2022 Potential hidden costs if dial back technology enabled at ARC level whilst international SIMs are being utilised

Appendix 5: Information process and technical architecture flow diagrams





For Advice and Further Information on Data & Cyber Security for TEC Services:

admin@tsa-voice.org.uk
01625 520320

TSA™

The voice of technology enabled care