The voice of technology enabled care

Practical Steps to Compliance: The End-to-End Resilience of Technology Enabled Care Solutions

Author: Steve Sadler – Head of Technology Strategy, TSA

Practical Steps to Compliance: The End-to-End Resilience of Technology Enabled Care Solutions Guidance:

Introduction

In the ever-evolving landscape of Technology Enabled Care, staying ahead of the curve requires a good understanding of the latest industry standards and best practices.

With this in mind, we present this document, 'Practical Steps to Compliance', with the requirements relating to the **'The End-to-End Resilience of Technology Enabled Care Solutions'**.

This document captures the main points of the guidance in an easy-to-understand format, distilling the terminology and insights in a step-by-step approach. Whether you are a seasoned Commissioner, a forward-thinking Service Provider, or an enthusiastic Supplier, we trust that the document will enhance your understanding of the main guidance.

The approach in steps:

Our approach to Resilience of TEC Solutions can be viewed in several steps.

STEP 1:

What is the service being delivered and is it fit for purpose?
Technology-Enabled Care comes in different forms; we may be helping people with emergencies and alarms in real-time, or we may be reaching out to people through proactive calls to check they are okay, or perhaps we are providing advice on lifestyle and wellbeing. These are all very important types of TEC support, but any short-term service failures would have very different impacts on the service users in each case. So, it is important that we start with a clear definition of what type of supportive service has been agreed with the users, and to keep things simple, we have defined three 'tiers' of services types, with examples, as follows

- Tier 1: Reactive, real-time and life-critical call handling, including telecare alarms, smoke detectors, fall detectors. Service failures for this tier would pose the greatest threats to life and limb.
- Tier 2: Proactive and personalised support, such as outreach check-in calls, medication reminders, activities of daily living (lifestyle) monitoring, and other services in response to a personal care plan.
- Tier 3: Preventative services, such as wellbeing apps, health questionnaires, advisory outreach services to a population of vulnerable people at risk. We could imagine that service users could tolerate longer disruptions to these services than for life-critical alarm calls.

We expect that providers of Services or Technology should be able to define the intended purpose(s) of the services being provided or supported, along with the anticipated impacts on health and care outcomes, and that this information should have been agreed with customers and users.

STEP 2:

How trustable does the service need to be? And how can we relate trust to measures of resilience?
If we are to place our trust in a service then, as a minimum, the service needs to:

- deliver the supporting services that were promised to the customers and users.

- be available and working when required, reflecting the urgency or importance of the desired outcomes.
- perform quickly enough to meet the desired response times.
- use information about users to deliver a quality service, whilst protecting that information.

We can define measures that relate to each of these aspects of trust, and collectively they provide a high-level description of the 'resilience' of any TEC solution.

STEP 3:

Identify a Design Authority, who has end-to-end responsibility for system resilience.

It is recognised that the delivery of TEC services can be complex, and a coordinated understanding of technology platforms, telecommunications, user devices, the associated data processing and skills requirements is needed to assure the end-to-end resilience of the service and underlying technology. Therefore, a single Design Authority (person or organisation) should be identified as the owner of this responsibility.

STEP 4:

Show that the target measures are achieved.

It is expected that the Service Provider, supported by their Technology Suppliers, will design and continue to monitor the performance of the service and underlying technology platform, to make sure it continues to meet the performance that has been promised to customers.

The minimum key measures that need to be achieved are as follows:

- **Data Protection & Security**

Self-certification against the Cyber Essentials scheme meets the minimum quality standard. Higher levels of quality compliance are possible, through independent evaluation or by certification against ISO27001. Compliance with the Data Security and Protection Toolkit (DSPT) Toolkit (or other UK equivalent) may be a requirement where services are provided to the NHS and organisations that are registered with a care regulator.

- **Availability of TEC Equipment & Monitoring (Annualised Availability)**

This is a key quality measure for any service, and it defines the extent to which TEC services are operational and useable when required. Availability defines the percentage of time for which the service is operating at its agreed levels of service performance and is fully accessible to users. For example, a service with 48 hours of 'downtime' per year is achieving 99.45% availability.

Any underlying technology platform that supports the service must deliver at least the same level of availability. The scale of the service also has an impact, since larger populations of end users increase the potential for loss of service actions per hour of downtime.

- **Maximum Single Instance Downtime**

A single and extended disruption can pose significant risks to end-users, and it will have a major impact on perceived service quality; The longer a service is down, the more likely that a critical service user will be unable to receive assistance within the "golden hour". Therefore, a quality measure is defined that relates to the maximum tolerable duration of any single disruption, in terms of downtime.

- **Transit Time from Alarm Activation to Response**

This measure covers the time from activation of consumer equipment to the presentation of associated information to the operators of monitoring service equipment. The required end-to-end performance is defined only for life-critical, reactive alarm calls.

Quality Levels Explained

An organisation that achieves the necessary requirements is rated as “Compliant”. However, some organisations may invest in higher quality levels that go beyond the “minimum” requirements. These different levels of quality are certified by audit and enable easy comparison of services by customers and users. The quality levels are defined as: “Compliant”, “Advanced Compliance” and “Outstanding Compliance”, and apply from November 2023.