Whitepaper
10_2020

IoT connectivity for telehealth and telecare

IoT enables ageing and vulnerable people to live richer, fuller, longer lives. Here's how to get the connectivity right to deliver on this promise.

Ref No: 9002

Welcome to the future of healthcare

Digital health, or telehealth, a thriving area of innovation, is changing how we treat and care for the ageing, sick and vulnerable. The latest sensor innovations allow people to live safe and full lives without constant human supervision. Digital monitoring of health conditions enables more personalised treatment and lifestyle recommendations.

These innovations rely on IoT devices, whether in homes or on the body. Such devices rely on good connectivity to securely transmit data to the device operator's cloud, where data is analysed in real-time, and life-improving recommendations made.

Getting this right allows ageing populations to live safely in their own homes for longer, improving their lives and reducing the burden on care industries.

These connected innovations present a huge businesses opportunity for tech companies, and cost reduction in health, care, and insurance. As populations age and more people live with chronic conditions and disabilities,[1] this is a rapidly expanding opportunity for both business innovation and social good. Ensuring such devices have the connectivity to reliably capture, share and analyse data is key to success.

1. Nearly 45% of 65–74 years olds have a disability, rising to 85% for those 85 and over. The 962 million people aged over 60 in 2017 is predicted to rise to 2 billion by 2050. See https://www.ageinternational.org.uk/policy-research/statistics/global-ageing/

– Digital health in the time of COVID-19

COVID-19 is accelerating digital health trends. There is already value in monitoring and communicating with the people in care. But when a deadly virus threatens the most vulnerable, this technology takes on a whole new significance.

Connected digital health devices allow those at risk to stay safe at home, whilst connecting them to the world. They allow carers to monitor health and intervene where necessary but eliminate non-essential visits. They allow people the freedom to go outside on their own. Some may even help detect or manage COVID-19 symptoms.

A large section of society, who a decade ago would need to move into care, can now live for many more years in their own homes thanks to this technology. Given the potential for viruses to spread in care settings, this could save many lives.

Section 1: The value of good connectivity to digital health and homecare

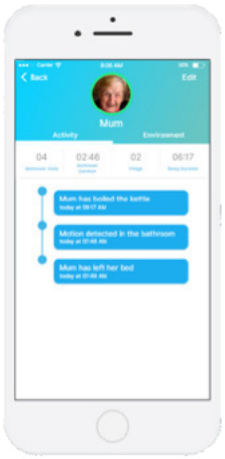
In this first section, we discuss why good connectivity matters across digital health and homecare. In the second section, we discuss how to get it right.

We look at three areas of digital healthcare where good connectivity is vital.

1. Passive monitoring

This involves connected devices in homes quietly monitoring patient's behaviour. Usually, the devices will not do anything or interfere, but critically they will spark action if they notice a concerning change.

Some may trigger an immediate response, e.g. a fall detector can immediately contact a care worker. Others may use more subtle indicators from data collected from multiple connected devices.



Alcuris's Memo Hub is a good example of the latter. The hub connects smart devices around a person's home, such as kettles and televisions, and backhauls this data to the Alcuris AWS cloud database, where it performs analytics to draw insights. This triggers alerts if their usual pattern of behaviour suddenly changes and can also monitor gradual changes which may indicate a need to review care regimes.[2]

2. For more information, see https://www.eseye.com/millions-of-vulnerable-people-to-benefit-from-new-iot-monitoring-service/

2. Active monitoring

This is where IoT devices necessitate proactive action from the resident or carer. Cameras or speakers in homes allow relatives or carers to check in at regular intervals. Panic buttons assure residents that someone will be there if they need them. IoT-enabled GPS pendants can be carried outside the home, providing a direct line to help, and a way for that help to locate them.

3. Condition monitoring

This final area involves monitoring health conditions on an ongoing basis, combining the first two approaches and usually involving more personal and detailed health data. This is used both in clinical trials to understand drug efficacy, and to monitor long-term conditions and treatment adherence.

Wearable movement detectors could be used to pick up subtle slowing movement in arthritis suffers. Diagnostic devices for blood pressure or fluid samples could monitor blood sugar levels in diabetics, or confirm medication has been taken, and upload them to healthcare databases. Many such offers combine sensors with self-reporting mechanisms, for example via a dedicated tablet device or software app.

An example is the **Philips Motiva** system, for patients with chronic conditions. This provides them with connected scales and devices to measure vital signs. The eCare companion tablet captures information via questionnaires and allows patients to monitor their condition and arrange video calls with carers. Due to the sensitive nature of the data, these devices are all managed through a single secure connected system, rather than utilising third-party devices.

Section 2: How to incorporate the right connectivity

All of the above situations involve collecting highly sensitive personal health data on which important decisions are made about people's lives.

It must be captured accurately, or the wrong conclusions will be reached, and it must work reliably or key data such as a distress signal may be missed.

The device manufacturer must consider privacy, security and ownership of the data, as well as how it is collected, transported and stored. In most cases that will mean designing the device (or suite of devices) to ensure high levels of control over data capture and transmission, and securely integrating that with cloud services where analytics can be performed.

None of this should come at a cost of usability. Such devices will usually be set up by a carer and used by people who have a low understanding of technology. Many will not know or wish to disclose their WiFi passwords and some may not have WiFi at all. These devices need to be extremely simple and intuitive.

1. Device design: Matching tech to application

Although connectivity can be implemented into existing devices (for which, skip to the next section), there is a strong argument for designing devices with optimum connectivity in mind from the start.

Consider how the device needs to be used. Many medical devices need to be lightweight, unobtrusive, robust and easy to use, or they will not be used correctly. This places some natural limits on design options which is not the case for larger or fixed pieces of technology.

There are choices to be made around connectivity that will dictate the optimum design.

If you have lots of connected devices, do you want to manage the whole connectivity path to each device individually with cellular modems, or is it acceptable to connect them all to a central hub e.g. using Bluetooth, WiFi Zigbee or a proprietary standard? The costs of individual cellular modems must be weighed against the costs of a hub, any certifications needed, and the management overhead at install, when the devices need to be paired, and over the lifetime of the product.

In the past, cost and power requirements of the modem often skewed design in favour of a hub. Older 2G modems demanded spikes of power and so needed high spec batteries. But newer communication protocols, such as Cat-M1, use lower power levels, allowing smaller batteries which may allow for other improvements in design, and make individual direct connections to each device more attractive.

Communication is not one way. If a device sends an alert, how can the person on the other end respond in a way that works for the user? IoT devices designed for younger users often communicate using text-based alerts, but older users may struggle with this. If they have a fall an hour's walk from home, a device which connects to a human voice will be far more reassuring than a line of text on their smartphone (if they have one). As networks around the world migrate users to LTE, this will drive the adoption of Session Initiation Protocol (SIP) clients (which allow users to make voice and video calls over the internet), within personal devices. Designers need to be aware of legislation for calls that terminate on public networks and ensure that their systems comply.

Finally, you need to think about what happens at the other end. Does it connect into a dedicated cloud service which analyses data and makes recommendations? Is there a person at the other end who needs to access data, in which case how should it be presented (a text alert, a dashboard or via an app)? Can that person respond directly through the system?

All of these decisions will affect how connectivity is incorporated, and hence the design, hardware, circuitry and power source.

Alcuris' Memo Hub Solution

2. Ensuring reliable connectivity

Whichever way you design the device, it will need to reliably connect to the internet so it can share its data with your cloud, and once analysed with the customer.

Devices designed for elderly and vulnerable people should be set up so that they work seamlessly out-of-the-box, automatically connecting to a mobile network without the need for complex setups.

They should be designed to work anywhere. They may be deployed around the country, from busy cities to remote villages, where there is no guarantee of WiFi availability. Some may be deployed across multiple geographies.

Mobile networks all have reception black spots and deploying thousands of devices across a country on a single mobile network will mean 15-25% devices might still be without a reliable connection. All culminating in some devices which fail to work for some customers or some that only work intermittently, or others which lose the connection altogether when the user goes for a short walk. Devices must be able to select the best network for that location and seamlessly change between them.

And this connectivity must be reliable and continuous. A dropped connection at a key moment could literally be a matter of life and death.

Ensuring connectivity is fit for purpose also involves testing it before deployment, to make sure it is behaving as expected and the tools for managing connectivity are effective within the device setup. Good testing involves putting the device in sandbox and simulating difficult network conditions, such as if the local mobile mast breaks, to confirm that the device recovers quickly, or identify changes if it does not.

3. Implementing adequate security

Finally, for devices handling sensitive data, end to end security is critical. Hardware, software and connectivity platforms all need to be secure for IoT devices to work effectively.

Many consumer SIMs lack advanced certificate-based security measures and send data over standard internet channels. This increases the risk of data being intercepted or lost. Dedicated solutions designed for secure applications offer better solutions.

Healthcare device manufacturers should take an end-to-end approach to security. This involves encrypting information at the device and communicating only via trusted private networks and secure gateways (i.e. private APN or VPN) which authenticate connections and ensure the service is authorised. Adding in tools which monitor data flows to detect unusual activity helps prevent malicious attacks.

Finally, we advise contracting a third-party pen tester to test any device before deployment.

How Eseye can help with digital health and homecare IoT

Eseye's **AnyNet+ eSIM** and connectivity technology provides a highly appropriate solution to the unique challenges faced by health and homecare IoT manufacturers, where users are widely dispersed and not tech-savvy. We ensure universal, ubiquitous connectivity and data security are built-in to your IoT device by design without any additional complexity for the user.

The eSIM can be programmed to detect and connect to the most available mobile network, and to switch network if the connection drops or the environment changes (e.g. the user goes for a walk and ventures into a black spot). It delivers continuous connectivity without dropping because our networking infrastructure is designed to provide highly available services – so no risk of dropped connections in an emergency.

This is true anywhere in the world, thanks to Eseye's relationships with over 700 mobile networks, allowing businesses to build connectivity into devices by design, and deploy a single product globally.

Our SIMs encrypt information and communicate only with Eseye's secure private access point name (APN). This authenticates connections and routes the data from the device to the cloud via trusted channels. It automatically integrates with trusted cloud services, such as AWS IoT Core, taking care of the complexity surrounding digital certificates. Using information gathered from our APNs we can feed data into analytics and AI engines which help to identify anomalies in behaviour.

Finally, **Eseye's consulting team** can help guide customers in every design decision throughout the process, from circuitry and component selection to device testing and simulation of challenging network conditions. All of which ensures devices are designed and proven for optimal connectivity whilst being fit for purpose, before they go into full production and extensive field trials.

Telehealth and telecare are critical industries that vulnerable, geographically dispersed people rely upon to keep them safe and healthy. Ultimately, ensuring every device has completely reliable, out-of-the-box connectivity will be key to industry growth, trust, and customer satisfaction.

No Limits.

To talk to Eseye about the issues raised in this whitepaper
or discuss the next generation of IoT solutions, please

@eseyem2m
Eseye
eseyeM2M
www.eseye.com