Implications of telemedicine in care homes: considerations for the evolving risk landscape

January 2023
Whitepaper

Produced in collaboration with:

BAYES BUSINESS SCHOOL
CITY, UNIVERSITY OF LONDON

LOCKTON®

Introduction

This white paper explores the evolving risk portfolio of care homes, as well as the risk management and insurance implications of introducing telemedicine into the care environment.

Telemedicine allows remote tracking and monitoring of patients' health data, gathering and securely transferring patient data to a cloud-based platform that is accessed by the relevant health professionals, detecting any irregularities and sudden changes in real time, as well as administering medication.[1]

With proven benefits during times of crisis, we have recently seen a higher dependence on telemedicine and telehealth technologies, which have helped ensure continuous healthcare provision. Earlier this year, Lockton published a white paper on cyber threats within care homes due to the advances in the application of Internet of Things (IoT) and medical technologies, which includes telemedicine. However, the associated exposures span beyond the cyber landscape, including potential medical malpractice exposures, as well as weakened patient-healthcare provider relationships and lack of trust in the quality of services provided due to the limited face-to-face interactions.

Evolving risk landscape

Increasing dependence on robust IT systems

While the application of telemedicine brings various benefits, it also triggers a change in the traditional risk landscape for care homes. To ensure adequate functioning, telemedicine requires quality and efficient internet connection – lagging sound and picture could lead to inaccurate information being supplied to healthcare providers, causing potential misdiagnosis and/or administration of wrong medication.[2]

Evidently, the implementation of telemedicine could trigger an array of IT issues, which increases the need for specialists to handle and manage the implemented technologies, to ensure the continuity and smooth operation. There is currently a gap in the required expertise and skillset to manage any emerging operational issues within care homes.

The sharing of data with other health professionals through common online channels and platforms, which is facilitated by telemedicine, creates a wider threat surface.

Cyber exposures

As discussed in our previous white paper, the increased dependence on IoT and telemedicine increases the risk of cyber threats for care homes. Organisations in this sector typically operate with modest cybersecurity budgets, limited IT support and outdated IT systems. Funds are often allocated towards operational necessities rather than cybersecurity measures and frameworks, making care homes a vulnerable target for cyber threats. Cybercriminals actively select organisations that are perceived as valuable or an easy target.

Care providers handle large volumes of personal and sensitive information relating to the residents, the residents' families, and other third-parties. Some of the information is highly regarded by cyber criminals as much of it is 'static information', i.e. information that cannot be changed, such as National Insurance numbers. This data commands a high price on the Dark Web, as they may be utilised for identity theft and other fraudulent activities.

The sharing of data with other health professionals through common online channels and platforms, which is facilitated by telemedicine, creates a wider threat surface. The networks may be used to gain access to larger healthcare organisations and governmental bodies, leaving the care homes vulnerable to liability claims. Telemedicine devices that are based on general-purpose operating systems (GPOS), such as smartphones, are particularly vulnerable to security threats given their dependence on third-party applications, which save and share the medical data. The varying security standards for these devices create risk exposures such as device loss/theft, app vulnerabilities and plaintext transmission.[3]

Furthermore, the use of telehealth technologies, such as wearable and ambient devices, which allow carers to monitor the health, safety, and wellbeing of the residents on a consistent basis (reducing the frequency of physical check-ups) is a risk. If those devices are connected to a server, cybercriminals can potentially hijack the devices, and disrupt their function. If a cyber incident were to occur, it may lead to a network outage, causing vital medical data to be inaccessible, including in the context of obtaining prescriptions. Unlike other sectors, where the impact of cyber events may typically include financial loss, business interruption or reputational damage, consequences in the care sector may extend to the health and safety of individuals.

Ethical concerns

Ethics is another prominent issue in relation to telemedicine. The lack of face-to-face interactions could lead to patient objectification, as they are perceived as an additional case to deal with rather than a suffering individual. The lack of proximity during service provision could lead to insensitivity on behalf of the healthcare provider, lack of attention, and misdiagnosis.[4] The potential loss of human connection and compassion due to the dependence on technologies for facilitating care is a major concern. To maintain quality of service provision for care home residents, it is important to ensure that there is consistency and continuity of medical and care providers. This includes regular follow-up sessions with patients after each consultation, to ensure comfort, progress, and recovery. The effectiveness of the uptake and delivery of telemedicine is also directly related to the user engagement, which can be facilitated by working with agencies that focus on digital inclusion through providing training and support.[5]

Further concern relates to overdependence on telemedicine to satisfy the varying needs and requirements of the residents. Telehealth technologies could be stigmatising for patients struggling with conditions requiring constant care and attention, as care providers become dependent on such technologies for monitoring the residents, reducing their personal interaction and consistent presence. One of the primary issues affecting the quality of services provided in care homes and the overall experience of the residents is the nature of care and support received. The established relationships between care workers and the residents have a considerable impact on residents' wellbeing and quality of life.[6] Maintaining such empathetic and intimate internal dynamics is crucial for ensuring quality and effective service provision.

Transparent and consistent communication is another factor affecting patient experience. Residents that do not receive the appropriate information and explanation in relation to the purpose of telemedicine technologies, such as wearables, may consider such devices as an invasion of their privacy and a form of surveillance – causing potential patient isolation.[7]

Legal factors

The legal aspect of telemedicine application is also an area of concern. As it stands, the regulatory system in the UK does not have specific laws and regulations governing telehealth and telemedicine. Therefore, this practice is regulated in the same way as traditional, non-digital, healthcare services.[8] The standards set for doctors by the General Medical Council (GMC), which doctors practising in the UK must be registered with, apply equally to remote and in-person consultations.[9]

Given the lack of specific regulation, various regulatory bodies have issued guidance to their respective professionals. Within this, the guidance provides high-level principles for remote consultations including: the prioritisation of patient safety, protection of vulnerable patients, attaining informed consent, undertaking of adequate clinical assessment, arrangement of after care, confirmation of adequate documentation and reporting, as well as keeping track of the evolving legal landscape.

Informed consent is another legal consideration, as legal allegations could arise from not informing patients about the risks associated with using telemedicine.

> It is crucial for care homes to seek professional advice on coverage and the required insurance arrangements to ensure adequate levels of protection.

Risk and insurance implications

Cyber risks and risk transfer

The dependence on the Internet of Medical Things (IoMT) and telemedicine coincides with the constant pace at which the Cyber space continues to evolve and develop. With the budding risk landscape and varying motives driving cyber-attacks, care providers are placed in a position to not only understand the nature and types of cyber risks they are exposed to, but also the gaps and weaknesses within their operational models. Care homes must now consider their approach across their strategic, operational, executional, and business risk.

Healthcare providers are not technology companies, although over the last two years we have seen a momentous shift in the adoption of technical and digitalisation; increasingly everything healthcare organisations now do is underpinned by technology. Cybersecurity is one of the foundations that underpins safe patient care, the reputation of the healthcare organisation, and the trust patients place in it. Ultimately, should technology fail, the resulting adverse consequences to the healthcare organisation may be very significant.

As cyber-attacks morph, cyber criminals find new ways to exploit vulnerabilities and avoid detection. In 2020, the NHS experienced a significant volume of cyberattacks, whereby 30,000 malicious emails were sent to the NHS in March and April, there was a 6,000% increase in "Phishing" incidents, and 51,910 signs of malicious activity were notified to the NHS by the end of August.[10] Hence, ensuring cybersecurity systems are in place, and that the staff are educated and supported to use them, is an essential part of the management of cybersecurity in today's environment. It is vital that care providers look very closely at their cyber hygiene protocols. Examples of good protocols include:

- Multi-factor authentication for remote access (MFA);
- An endpoint detection and response (EDR) solution rolled out across the IT environment;
- Privileged access management (PAM) and permissions across the IT environment;
- Secure offline backups;
- An Incident Response Plan specific to ransomware that is updated and tested regularly;
- A Business Continuity Plan addressing network outages, off-line communication, and data recovery protocols;
- Remote desk protocol access from outside the network;
- Updated software and patching protocols;
- High-level employee awareness training;
- Password management software;
- Vulnerability assessments, including penetration testing, red-teaming, and table-top exercises; and
- Appropriate separation of Operational Technology and Information Technology.

Understanding the key threats is crucial for implementing the appropriate cybersecurity measures within care homes, which may include:

- Storing sensitive information and data
- Website security vulnerabilities
- Internet of Medical Things (IoMT)
- Internet of Things (IoT)
- Operational Technology
- IP
- Contracts
- People

Cyber risk management and insurance

An important risk mitigation process is the transfer of risk to insurance. The current state of the Cyber market continues to endure a challenging phase of corrections, responding to a claims environment that is highly active and costly, with a constantly changing threat landscape. As insurers look to adjust their books in line with new requirements, the scrutiny applied by underwriter remains to be high. Today's marketplace demands the very best intermediary expertise and leadership to help businesses secure the coverage that meets their needs and demands. The process of obtaining insurance requires onboarding services, strong partnerships with experts, unrivalled relationships with insurers and, in the event of a cyber incident, the best minds in the business to help guide firms through to a quick and full recovery.

The insurance process

Insurer requirements vary and continue to evolve with changing sets of questions relevant to the current threat landscape and outlook. Brokers will often collate insurer requirements to form a multi-page application; during which information gathering begins. Ultimately the proposal form acts to understand a client's requirements and current Cybersecurity posture, assessing whether a firm has a healthy and secure network. Generally, insurers will want to know how care homes are operating in the following areas:

People risk

- Training and awareness
- Access control

Operational risk

- Governance frameworks
- Policies and procedures
- Management of vendors
- Management systems
- Audit regimes

Technological risk

- System design
- Software configuration
- Encryption protocols
- Detection and monitoring

The rise of ransomware has been one of the most important cyber developments in the market, bringing about a vast change to the frequency and severity of attacks. With ransomware attacks occurring every 11 seconds on average, almost every organisation is now at risk, irrespective of size and sector. It is now not a question of "if" but "when". With ransomware being one of the leading loss drivers within the cyber market insurers have brought new rates to the forefront, causing the following responses from cyber underwriters:

- Increased retentions
- Coverage is often restricted by the inclusion of ransomware-related sub-limits and coinsurance (or both)
- Where sufficient cyber hygiene controls are lacking, ransomware related exclusionary language is increasingly common
- Minimum rate increases, even for clean risks with best-in-class controls
- Supply chain exposure is causing reverberations around the marketplace and sharpening underwriter focus
- Additional questions are being asked of clients specifically in relation to their exposure to the Accellion, Microsoft Exchange, SolarWinds, Kaseya and Log4j events.

Greater scrutiny around security controls, which mitigate the ransomware threat, are also front and centre of the insurers' underwriting process. Hence, regardless of the origin of cyber exposures, implementing a robust cyber risk management framework is crucial for care homes, to both increase their organisational resiliency and ensure operational continuity, as well as secure the appropriate terms and coverage from the insurance market.

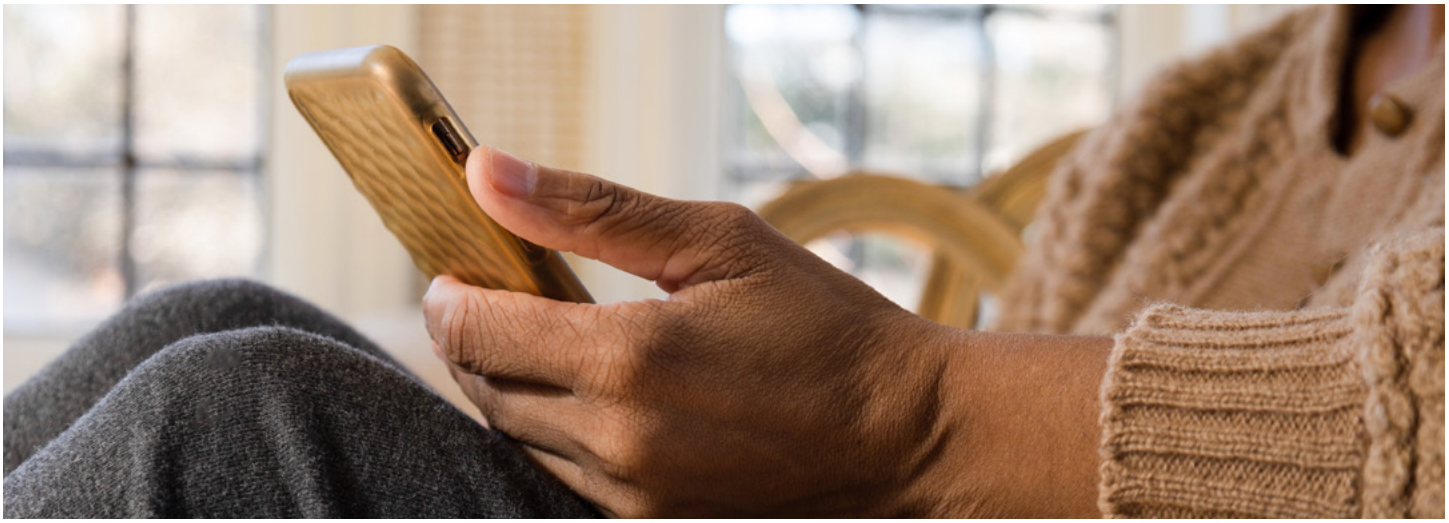
Medical malpractice

In the past, the telehealth services provided were less complex, which lowered the associated medical malpractice risk. However, as the dependence on telemedicine evolves and the nature of the technologies utilised become more sophisticated, the risk is likely to increase. As discussed, whilst telemedicine potentially increases efficiency and quality of service provision, there are several concerns regarding the lack of human interaction, overreliance on the output from the utilised technologies, and potential oversight.

Care homes are a haven for vulnerable individuals that often require consistent attention, support and care. System outages, products failing to perform, technology errors and omissions and generally poor infrastructure are only a few challenges faced by those providing digital health services. Deletion of crucial information relating to a symptom, or the quality of an image submitted can result in a misdiagnosis and potential large liability losses. This could also result in inappropriate levels of medication being administered by care givers, or having the wrong medications prescribed, also leading to liability claims. Furthermore, depending on indications from monitoring technologies for any signs of irregularities, rather than ensuring consistent physical check-ups could result in delayed detection of serious conditions, which may be due to faulty equipment or delayed data transmission due to poor connection. These rare circumstances could result in death or injury of the resident.

Although telemedicine in care homes has limited use, from a diagnostic and treatment perspective, it is significant from a risk prevention aspect. Being able to detect any abnormalities or accidents (ex. a resident has a fall) real-time will help care givers proactively prevent incidents from escalating, potentially worsening existing medical conditions or giving rise to new injuries etc. This could help decrease the likelihood of claims arising from negligence and errors in care provision.

It is crucial for care homes to seek professional advice on coverage and the required insurance arrangements to ensure adequate levels of protection. The markets will expect robust governance and policies to be in place, which could often be complex and time consuming without the guidance of subject matter experts. Medical malpractice policies require an extension to cover the systems used, i.e., extending the coverage to include the implemented technologies, as well as the actions taken by healthcare providers. Extending coverage to include the systems and technologies will reduce the likelihood of a dispute arising from a claim as to which policy should respond, as telemedicine care is viewed holistically alongside traditional practices.



Considerations

- **Establish a robust enterprise risk management (ERM) approach, which addresses both evolving and emerging risks.** Care homes should consistently identify, assess, and mitigate all risks threatening their continuity, quality of service provision, and most importantly, the health and safety of their residents. Enforcing a strong internal risk culture, which promotes transparent communication across all stakeholders, will facilitate the risk management process, as well as ensure the appropriate implementation and monitoring of the risk controls and measures.
- **Robust operational continuity planning.** Due to the increased dependence on IT systems and the smooth operation of the implemented telemedicine technologies, contingency planning is crucial for ensuring continuous service provision.
- **Consistent internal training to address any vulnerabilities and limit the potential exposures.** This should include enhancing internal knowledge regarding cyber security and hygiene, as well as how to operate the implemented technologies safely.
- **Transparent and regular communication with subject matter experts and risk advisors is necessary.** To ensure you are adequately prepared for the underwriting process, and that your requirements and needs are adequately reflected in your insurance arrangements, you need to engage with your insurance brokers early on in the process. Preparation and timing for certain markets is paramount, especially for the Cyber insurance market.
- **Acquire the appropriate skillset to manage the applied technologies and software facilities.** IT professionals and telemedicine experts should be readily available, to ensure continuous and efficient performance and functioning, as well as promptly handle any issues that could disrupt the provision of services or pose a risk on the health and safety of the residents.
- **Transparent and consistent communication between care providers, the residents, and other relevant individuals, such as the residents' relatives.** Ensuring that the residents are consistently satisfied and comfortable with the services provided is a priority for care homes. When implementing innovative and novel solutions, which the residents lack the knowledge and understanding for, it is important to inform them about the benefits and risks of using such technologies. Care providers should also seek their residents' consent for using such technologies, as any sudden changes in the mode of healthcare service provision could cause distress and discomfort. Learning how to safely use certain devices, such as wearables, is also key, as it also ensures the residents' safety.
- **Keep up with the evolving legal landscape and regulatory requirements.** The laws governing the use of telemedicine is ever-changing; therefore, it is crucial for care providers to stay alert to any changes to avoid the risk of non-compliance and regulatory scrutiny.
- **Telemedicine technologies are meant to increase efficiency and quality of care, but not replace human intervention and responsibilities.** As mentioned, overreliance on the implemented technologies might create a barrier between care providers and the residents, as the level of physical interactions decrease. Care providers should stay attentive to body language and physical cues, to detect any irregularities or changes in behaviour that could signal discomfort.
- **Thoroughly understand the extent of your digital offering, as insurers will require more information on your telemedicine applications.** To better understand your risk as a care home, insurers are likely to ask about how digital consultations are used, whether the used technologies are subcontracted or internally owned and offered, the precautions and training undertaken to ensure smooth and safe application, the available expertise to manage the implementation and maintenance of the technologies, the geographical boundaries of the services received remotely (where are the doctors located in relation to the patient), as well as how is the data accessed, protected and shared/ transferred etc.

References

1. Hedges, L., 2020. 3 Types of Telemedicine and How They Each Improve Patient Experience. [Online] Available at: https://www.softwareadvice.com/resources/types-of-telemedicine/.

2, 5, 7. Olwen E Williams, S. E. C. S. J. C. W. J. W., 2017. The use of telemedicine to enhance secondary care: some lessons from the front line. Future Healthcare Journal, 2(4), pp. 109-114.

3. Dong-won Kim, J.-y. C. a. K.-h. H., 2020. Risk management-based security evaluation model for telemedicine systems. BMC Medical Informatics and Decision Making, 20(106).

4. Giulio Nittari, R. K. S. B. G. P. G. B. A. S. F. A. a. G. R., 2020. Telemedicine Practice: Review of the Current Ethical and Legal Challenges. Telemedicine and e-Health, 26(12), pp. 1427-1437.

6. National Institute for Health and Care Excellence, 2019. People's experience using adult social care services [QS182]. [Online] Available at: https://www.nice.org.uk/guidance/qs182/chapter/quality-statement-3-continuity-of-care-and-support

7, 8. Taylor Wessing, 2022. Issues with regulation of telemedicine in the UK. [Online] Available at: https://www.taylorwessing.com/en/insights-and-events/insights/2022/06/issues-with-regulation-of-telemedicine-in-the-uk

10. BSI (2022). Cybersecurity in the age of Telemedicine. Retrieved from https://www.bsigroup.com/en-GB/healthcare/digital-healthcare/cybersecurity-in-the-age-of-telemedicine/

Get in touch

To learn more about any of the information above, or to find out how Lockton can help you mitigate these risks, please do not hesitate to get in touch with us.

Contact

Flora McCabe
Head of Advocacy and Risk Management - Healthcare Lockton Companies LL

E: flora.mccabe@lockton.com

Lucy Scott
Partner - Cyber and Technology Lockton Companies LLP

E: lucy.scott@lockton.com

Authors

Reem El Khatib
Risk and Research Manager Lockton Companies LLP

E: reem.elkhatib@lockton.com

Aishwarya Vinny
MSc Insurance and Risk Management Bayes Business School

Dr Cormac Bryce
Course Director, MSc Insurance and Risk Management Bayes Business School

Independence changes everything

10834