IT Needs of Care Homes

Executive Summary

- The purpose of this document is to provide an overview of reliable, secure IT systems for the delivery of safe and compliant care to individuals in residential care homes.
- Care homes handle sensitive patient data and must comply with the General Data Protection Regulation (GDPR) as outlined by the UK Government.
- There are some basic requirements (such as secure WiFi networks, encrypted devices, and regularly backed-up data) that should not be negotiable in any care environment.
- The organisation's care management systems must be secure and have a support mechanism in place, as well as be backed-up regularly.
- A variety of cybersecurity controls should help prevent data breaches and ransomware attacks from occurring.
- CCTV systems, VoIP (voice over internet protocol) communication systems and remote access solutions should be properly configured according to the law and regulations of the Information Commissioner's Office (ICO), NHS Digital Security Policy Toolkit (DSPT), and Care Quality Commission (CQC).
- Utilising a structured, 30-day improvement plan will give the organisation a strong foundation to continue developing its resilience.

Who This Guide Is For

This guidance has been created for:

- Providers of care home services in the UK
- Registered Managers
- Operations Managers
- Directors of small and medium-sized care providers
- Non-technical decision-makers responsible for compliance and quality with respect to information technology and data management and security (where applicable)

No expertise in IT is required to follow this document.

What You’ll Achieve

When you have completed this guide, you will:

- Be able to comprehend the foundations of IT that modern care home operators rely upon
- Know what expectations regulators have in relation to data management and security
- Be able to identify practical and affordable ways that you can improve the management of data at your care home
- Have an improved understanding of how to reduce the risk of a data breach or loss of system access during downtimes from IT failures

- Be better prepared for your next care home regulatory inspection
- Receive a checklist of actions to take within the first 30 days of completing this guide

Why IT Matters in Modern Care Homes

Digital systems have become vital for providing care home services by supporting:

- Electronic care plans
- Electronic medication administration records (eMAR)
- Staff schedules (rosters)
- Incident reports
- Communication between care homes and GPs/hospitals
- Communication portals for families
- CCTV systems for safeguarding

Care homes process very large quantities of "special category data" (health information) that are subject to enhanced levels of protection under the UK General Data Protection Regulations.

The Information Commissioner's Office (ICO) has made it clear that specific protection is required for health data.

Where care homes connect with NHS systems or manage NHS-related data, the NHS Data Security and Protection Toolkit (DSPT) may also apply.

The Care Quality Commission (CQC) is increasingly requiring care providers to demonstrate that they operate safe, secure, and well managed digital systems as part of its "Well-Led" domain requirements.

Core IT Requirements for Care Homes

1. Secure & Trustworthy Wi-Fi

What does this mean?

- A well-designed wireless network for all resident areas (including staff areas and office areas).

Why is that important?

- To support digital care systems
- To support staff moving around
- To enable family communication
- To support new types of communication systems, including modern call systems

Minimum Standard:

- Router/firewall device suitable for business use
- Separate networks for staff and residents

- Strong password for Wi-Fi network
- WPA3/WPA2 security

Better Standard:

- Router/firewall device with managed security and intrusion prevention system
- VLAN segmentation between Care Systems, Guest Wi-Fi, and CCTV
- Wi-Fi Coverage Survey conducted

Quick Wins:

- Set up separate guest Wi-Fi right away
- Change router's default password
- Disable obsolete security/encryption

2. Staff Devices (Laptops, Tablets, Smartphones)

What does this mean?

- Secure devices (laptop, tablet or smartphone) typically used by care staff/management.

Why is this important?

- All devices contain a lot of sensitive information:
- Resident health information
- Incident reports
- Employment information

Minimum Standard:

- Encrypted devices
- Strong password with multi-factor authentication
- Business class/commercial grade antivirus
- Auto-updates (where supported)

Better Standard:

- Mobile Device Management (MDM)
- Remote wipe capability
- Centralized monitoring of devices

Quick Wins:

- Enable encryption (e.g., BitLocker, FileVault) on all computers/laptops
- Enforce strong password and multi-factor authentication on all care software use
- Remove access of any former employees to any company systems/devices

3. Software for Care Management

What This Is

- System that electronic care planning as well as record-keeping.

Why This Is Important

- Enables improved audit trail.
- Creates fewer errors in paperwork.
- Helps to support CQC inspections that require paper trails.

Minimum Standard

- Using a reputable provider has to include:
- Cloud-based and UK-based provider
- Creating Data Processing Agreement
- Enabling MFA

Better Standard

- Integration with eMAR.
- Secure family portal for residents/clients.
- Role-based security access controls.

Quick Wins

- Confirm DPA signatory
- Review number of active users on the system
- Enable Activity Logs for users of the system.

4. Backup & Business Continuity

What This Is

- Copy of essential data that are stored securely.

Why This Is Important

- Because if there were to be a Ransomware attack or the system falls over then all operations would stop

Minimum Standard

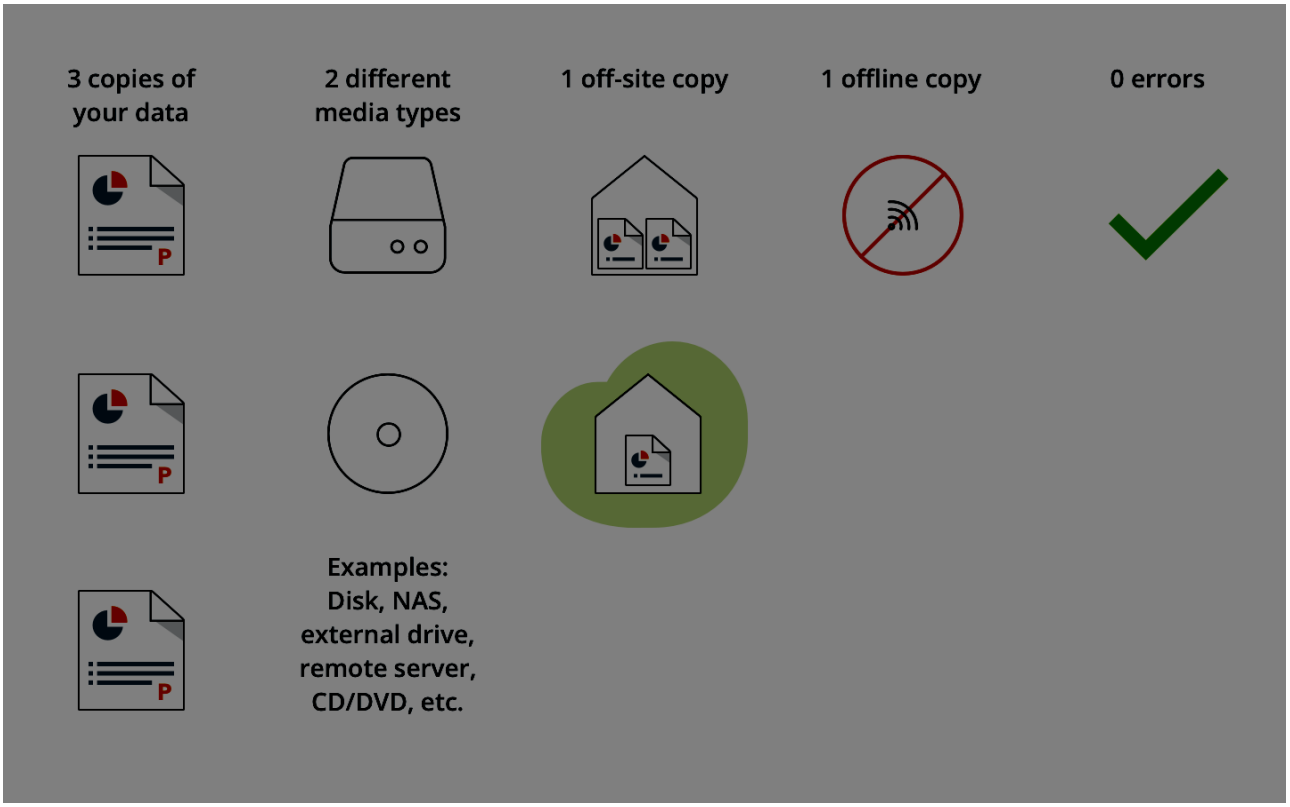
- Daily automated backups are carried out.
- Off-site copy of backup data is kept.
- Test restore data on a quarterly basis.

Better Standard

- 3-2-1-1-0 Backup Rule
- Immutable Cloud Backups
- Documentation for disaster recovery including business continuity plan.

Quick Wins

- Confirm Last Successful Backup.
- Perform one test data restore during this month.
- Ensure backup administrator has MFA enabled for account.



5. Cyber Protection

What This Is

- Security measures used to create a layered security system for protecting systems of care.

Why This Is Important

- Care home facilities are often targeted by phishing attacks.

Minimum Standard

- Business antivirus or EDR.
- MFA on email and care software.

- Robust password policy.
- Firewall Protection for endpoints that connect to outside networks.

Better Standard

- Managed security monitoring.
- Conduct training for staff on phishing awareness.
- Have an incident response plan in place.

Quick Wins

- All users are required to enable MFA.
- Basic phishing awareness training for all staff members.
- Remove any inactive or unused facility user accounts.

6. CCTV Systems

What It Is

- Security and protection through surveillance methods.

Why It Matters

- CCTV is a system that collects private data so it must comply with the UK GDPR.
- The Information Commissioner's Office creates guidelines around CCTV.

Minimum Standard

- Visible signage
- Stored securely
- Limited access
- Has a set retention period

Better Standard

- Encrypted storage
- Logging of access
- A written CCTV policy

Quick Wins

- Review retention period
- Limit Administrative access
- Ensure lawful basis has been documented

7. VoIP & Communication Systems

What It Is

- Cloud-based telephone systems.

Why It Matters

- Communication with customers
- Emergency call handling
- Home working

Minimum Standard

- VoIP system suitable for business use
- Strong passwords for administration
- Configured correctly on network

Better Standard

- All communication between VoIP phones is encrypted
- VoIP traffic is kept separate from other network traffic
- Provided with a backup internet connection

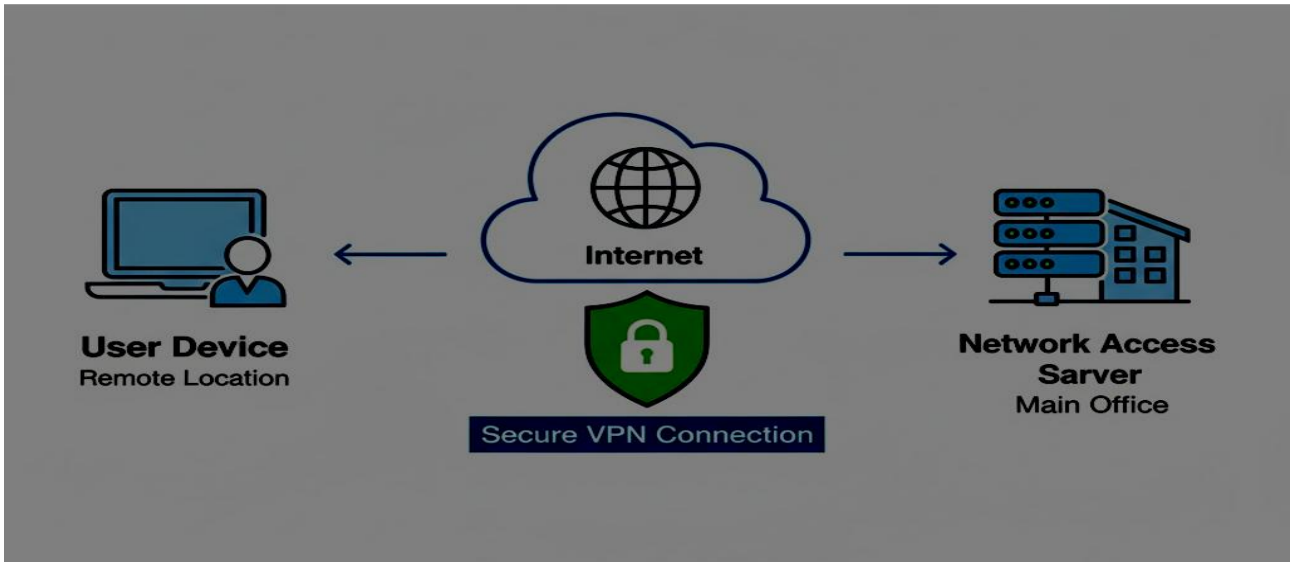
Quick Wins

- Reset all default VoIP passwords to something secure
- Limit outside access

8. Remote Managers Access

What It Is

- Access to IT systems securely from outside of the location.



Why It Matters

- Useful to the employee but extremely high risk if the system has not been secured.

Minimum Standard

- Should have two forms of security, VPN connection and multi-factor authentication.
- It should be based on each employee’s role within the company.

Better Standard

- Should have Conditional Access Policy applied.
- Should be able to check devices for compliance.

Quick Wins

- Disable any RDP connections that are open
- Make sure the VPN is required when accessing off-site.

Cybersecurity & Data Protection in Care Settings

The handling of personal health information is typical for care homes. Under UK GDPR:

- You are considered to be a data controller.
- Personal health information is classified as a special type of data.
- It is essential to provide suitable protections for that information.

The Information Commissioner's Office may ask you to report on certain breaches within 72 hours of discovery.

If you are using NHS-affiliated systems then you may be obligated to follow standards set by the DSPT.

The CQC will consider the following in their inspections:

- Data governance
- Security measure effectiveness
- Incident management

At a minimum, there are required documents for data governance that include:

- Data governance policy
- Breach response plan
- Privacy notice
- Staff training documentation

20-Bed Care Home Scenario

This care home is a smaller-sized residential facility.

Challenges:

- Limited budget
- One Internet line
- Many paper processes

Actions Taken:

- Upgraded to business-grade Wi-Fi.
- Implemented cloud-based care management software.
- Enabled multi-factor authentication (MFA)
- Implemented daily cloud backups to protect data loss.

Outcome:

- Better prepared for inspections; less paperwork processing errors.

50-Bed Care Home Scenario

This care home is a larger nursing home.

Challenges:

- Dealing with high volumes of data
- Monitoring all areas of the home via CCTV
- Integration with NHS systems

Actions Taken:

- Network separation
- Use of a managed firewall
- Encrypted data backups
- Quarterly evaluations of the care home's network security

Outcome:

- Improved resilience; aligned to DSPT standards.

30-Day IT Improvement Checklist

Days 1-10: Immediate Security

- Activate Multi-Factor Authentication
- Replace Default User IDs and Passwords
- Verify Compliance with Backup Procedures
- Isolate Guest Wireless Network

Days 11-20: Strengthening Systems

- Audit Care Software Access Permissions
- Ensure Encryption on Devices
- Update Firewall
- Establish Breach Reporting Procedures

Days 21-30: Governance and Compliance

- Provide Staff Training
- Ensure Compliance with CCTV Regulations
- Test Restorability of Backups
- Perform Annual IT Review

Frequently Asked Questions

1. **Will Cybercriminals Target a Care Facility?**

Yes, especially using phishing attacks.

2. **Is the NHS Digital and Cyber Security Policy Mandatory to Follow?**

This is dependent upon whether the individual or organisation accesses NHS systems.

3. **Do We Require a Full-time IT Manager?**

Generally, no; most organisations use some sort of managed services providers for their IT needs.

4. **How Often Should Backups be Made?**

At least daily.

5. **What Will Happen if We Lose the Data of a Resident?**

You may have to report the incident to the ICO (Information Commissioner's Office).

6. **Is Cloud-Based Care Software Secure?**

As long as it is implemented properly and from a trusted vendor.

7. **Do Staff Have to Complete Cybersecurity Training?**

Yes, at a minimum every year.

8. **Is It Difficult to Use Encryption**?

No; there are many tools available already built-in.

9. **What is the Biggest Risk to Care Facilities?**

Phishing scams and weak passwords.

10. **Are Improvements Able to Be Made Over Time?**

Yes; there is a structured plan available to be used.

About This Guide

The **Computer Support Centre** is a UK-based IT & Cybersecurity Consultancy headquartered in the UK with over 15 years experience of delivering support to care homes and care providers. Our focus is on practical, compliant IT solutions that reflect the operational realities of the care sector.

Our goal is to provide clear, plain-English guidance to assist owners and managers of care homes with understanding what they really need, prioritising improvements and implementing cost-effective controls to improve security and build resilience and regulatory confidence.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

Today’s Care Homes rely on dependable and trusted IT systems for delivering safe, high-quality services to clients. Application of Wi-Fi, care management software, backup systems, cybersecurity and other technical components create the solid foundations required to protect both the client and the business from harm.

Both UK data privacy law (UK GDPR), the information commissioner's office (ICO), NHS Data Security Protection Toolkit (NHS DSPT where required) and Care Quality Commission (CQC) have numerous guidelines on meeting the above. However, you don’t need complex or expensive systems in order to comply; rather it is a matter of having proportional controls, clear policies, and regularly reviewing these areas.

The ability for Care Homes to implement realistic or practical improvements in each of the above areas will enable them to strengthen their security posture, be better prepared for inspection readiness, and offer caregivers & clients confidence in providing continuity of care at the end of the 30-60-day processes described above.