

Academic Information

- ▶ **Module Title and Code:
Digital Skills and Research
Methods LCHS4007_BIRM**
- ▶ **Group Members:**
 1. Tasmia Bibi -2435170
 2. Mary-
 3. Jannatul Ferdous -2519627

Digital Safety Action Plan for Greenfield Home Care Agency

Digital technologies are widely used in homecare services to support communication, record keeping, and care delivery. While these technologies can improve efficiency and coordination of care, they also introduce risks related to data security, privacy, and patient safety, particularly in homecare settings where staff work remotely.

This assignment focuses on Greenfield Home Care Agency and aims to develop a Digital Safety Action Plan to support the safe, ethical, and effective use of digital systems. The plan addresses key areas such as secure system access, safe digital communication, data management, and compliance with UK data protection regulations to protect patient information and maintain care quality.



1. What is Digital Safety & Why It Matters

1.1 What is Digital Safety?

- The practice of protecting personal data and devices while using the internet

Digital safety refers to the protection of digital systems, devices, and data used in care services (Flott, Maguire and Phillips, 2021). In a homecare agency, digital safety means ensuring that patient information is kept confidential, digital records are securely stored and accessed, and technology is used responsibly by staff. It also includes protecting systems from cyber threats, preventing data misuse, and ensuring that digital tools do not cause harm to service users.



1.2 Why Digital Safety Matters in Homecare?

- Strong digital safety supports trust, privacy, and care quality.
- Protects patient confidentiality and sensitive health data
- Reduces the risk of data breaches and cyberattacks
- Ensures safe remote working for homecare staff
- Prevents misuse or unauthorized sharing of digital information
- Maintains trust between service users and care providers
- Supports safe, ethical, and high quality homecare

2. Digital Safety Action Plan

Research shows that poorly managed digital technologies can increase risk rather than improve care, making digital safety essential for protecting vulnerable individuals and maintaining high-quality, ethical homecare services (Powell et al., 2016; Hamblin, 2020; Hamblin, Burns and Goodlad, 2023).

The use of digital systems also creates risks related to data privacy and security. Protecting patient information is essential to maintain public trust in healthcare organization .

This assignment aims to explore digital safety within homecare services and to develop an evidence-based digital safety action plan for Greenfield Homecare Agency. The key goals of this assignment are:

2.1 Secure Access

As staff use Microsoft 365 to access care records, schedules, and internal documents, it is essential to ensure that only authorized personnel can access sensitive information. This goal focuses on reducing the risk of unauthorized access through secure logins, strong passwords, and controlled user permissions. (Powell et al. (2016)

Following actions can ensure security and Prevents unauthorized access to patient data -

- Strong passwords
- Role-based access
- Secure logins for staff device

2. Digital Safety Action Plan Cont.

2.2 Email Awareness

Email is commonly used by staff at Greenfield Home Care Agency to share information and communicate with colleagues. However, emails can also create risks, such as phishing attacks or accidental sharing of confidential patient information.

Digital risks often come from how systems are used, not the technology itself so , following action can help in mitigating risks and Reduces errors and unsafe digital practices -

- Regular staff training
- Clear guidance on using digital systems .

2.3 Data Management

Safe data management is important in homecare services where patient records are accessed and updated digitally. At Greenfield Home Care Agency, digital care records and shared documents must be stored and handled carefully to protect patient confidentiality.

The importance of knowing how data is stored and shared. Secure storage of patient records and controlled data sharing help protect confidentiality and support safe digital care practices (Goundrey-Smith, 2019).

2. Digital safety action plan Contd.

Following actions can protect confidentiality and improves continuity of care –

- Safe data sharing
- Safe care depends on accurate and secure transfer of information across settings.
- Secure communication channels
- Clear rules for sharing patient data

2.4 Confidentiality and Compliance

This goal calls for clear responsibilities in digital healthcare systems. By training staff and enforcing confidentiality policies, homecare agencies ensure ethical and responsible use of patient data

UK Data protection Regulations -

The final goal is to ensure confidentiality and compliance with UK data protection regulations within Greenfield Home Care Agency. As the organization handles sensitive personal and health data, it must comply with GDPR and professional care standards. This goal aims to ensure that digital technologies are used ethically and legally while maintaining trust between the agency and service users.

3. How can DSAP be improved?

My action plan is support a digital health systems that must protect patient data and clearly define responsibilities. This is especially important in homecare settings where staff work remotely and manage sensitive information. Staff need to understand where patient data is stored and who can access it. Secure storage of patient records and controlled data sharing help protect confidentiality and support safe digital care practices.

Based on the BMC Geriatrics research paper -UK. BMC Geriatrics, 25(875).

- ❑ Homecare staff rely heavily on digital tools . (UK. BMC Geriatrics, 25(875))
- ❑ Handling patient data outside offices increases risk
- ❑ Digital safety depends on staff training and clear rules Strong digital safety supports trust and quality of care

Problems

- ▶ Digital homecare systems depend on reliable internet, power supply, and secure networks, otherwise care and emergency responses can fail.
- Many digital devices do not meet the same safety standards as traditional alarm systems.
- Data collected by smart devices (voice assistants, monitoring tools) raises privacy, consent, data security concerns, especially for vulnerable people.
- There is low awareness among users and staff about how data is stored, shared, or used.
- The need for clear governance, updated safety standards, and ethical data handling in homecare (Hamblin,2021).
- Technology can improve care, but without strong digital safety frameworks, it can put service users at risk.

4. Application to Greenfield

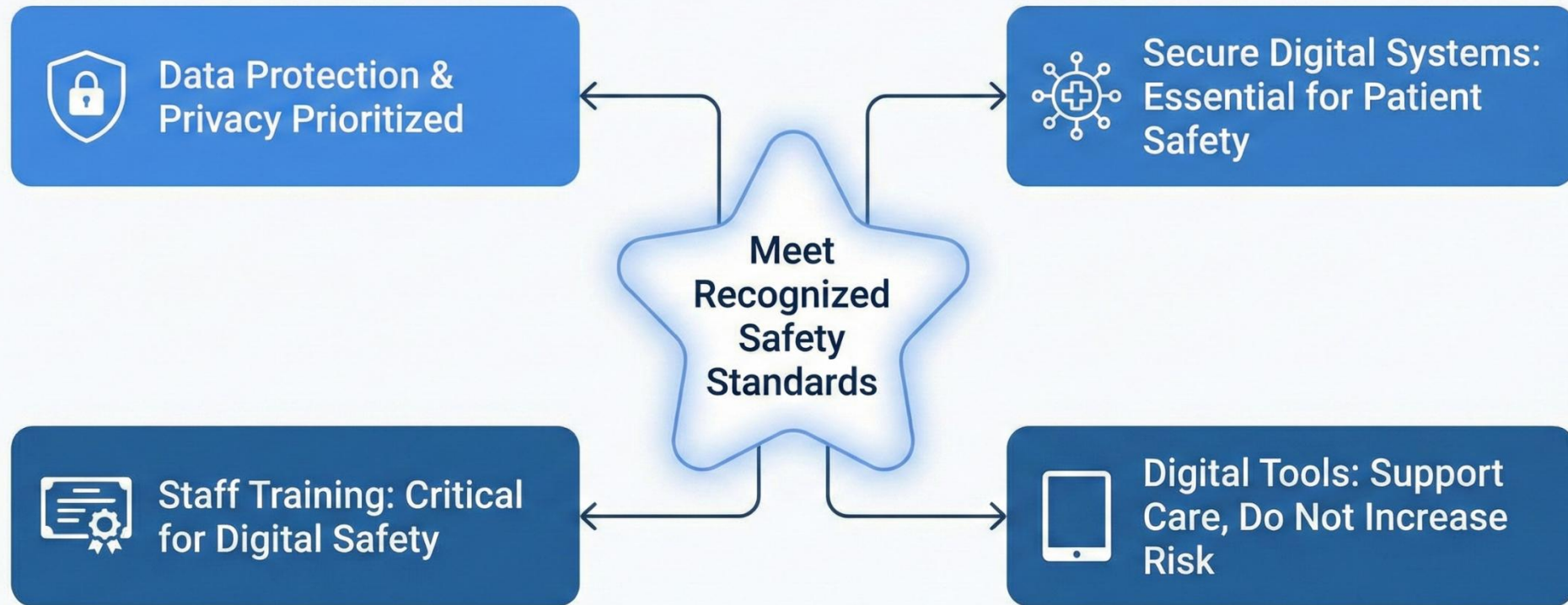
This research shows that digital systems can improve safety and efficiency in care services, but only when –

- information is accurate, secure, and shared appropriately. In a homecare agency like Greenfield, where staff work remotely and rely on digital records, strong digital safety measures are essential to protect patient data and support safe care delivery (Goundrey-Smith, 2016)
- Secure access to digital systems
- Safe use of email and communication tools
- Secure storage and management of patient data
- Confidentiality and GDPR compliance



4. Application to Greenfield Home Contd.

5 Key Pillars for a Secure Digital Action Plan in Greenfield Homes



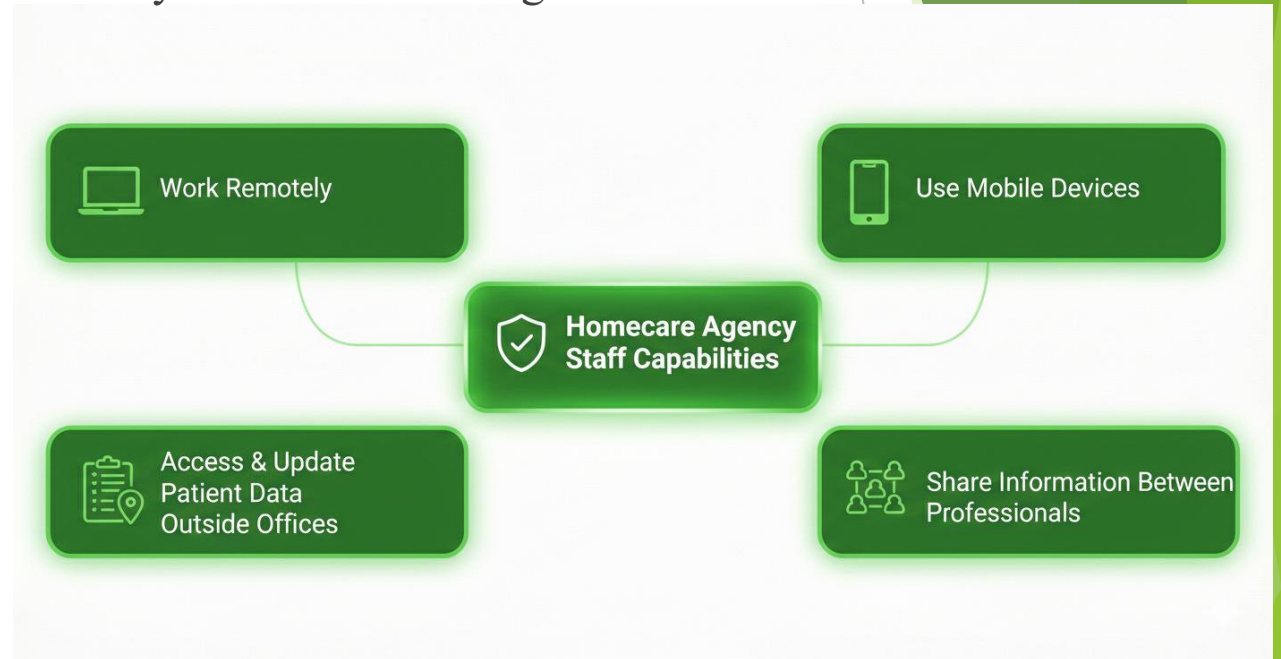
5. Benefits of the Action Plan

Digital technology improves safety only when digital safety controls are strong.

What this means for a homecare agency?

In a **homecare agency**, staff can:

- ▶ Work remotely
- ▶ Use mobile devices
- ▶ Access and update patient data outside offices
- ▶ Share information between professionals



According to **Alotaibi and Federico (2017)**, when digital information is not accurate, secure, or clearly transferred, patient safety can be affected. This makes digital safety especially important in homecare settings.

References

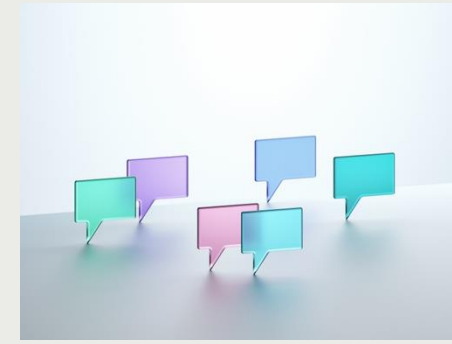
- Alotaibi, Y.K., Federico, F., 2017. The impact of health information technology on patient safety. *Saudi Medical Journal* 38, 1173-1180. <https://doi.org/10.15537/smj.2017.12.20631>
- Bende, P., Vovk, O., Caraveo, D., Pechmann, L., Leucker, M., 2023. A Case Study on Data Protection for a Cloud- and AI-Based Homecare Medical Device, in: *Lecture Notes in Computer Science*. pp. 138-161. https://doi.org/10.1007/978-3-662-68191-6_6
- Flott, K., Maguire, J., Phillips, N., 2021. Digital safety: the next frontier for patient safety. *Future Healthcare Journal* 8, e598-e601. <https://doi.org/10.7861/fhj.2021-0152>
- Goundrey-Smith, S.J., 2019. Technologies that transform: digital solutions for optimising medicines use in the NHS. *BMJ Health & Care Informatics* 26, e100016. <https://doi.org/10.1136/bmjhci-2019-100016>
- Hamblin, K., Burns, D., Goodlad, C., 2023. Technology and homecare in the UK: Policy, storylines and practice. *Journal of Social Policy* 54, 412-428. <https://doi.org/10.1017/s0047279423000156>
- Igboko, U.A., Temitope, O.A., 2025. Securing Public Health in The Digital Age: A Cybersecurity Case Study of UK Local Council Health Services. *International Journal of Scientific and Management Research* 8.
- Powell, J., Newhouse, N., Boylan, A.-M., Williams, V., 2016. Digital health citizens and the future of the NHS. *Digital Health* 2, 2055207616672033. <https://doi.org/10.1177/2055207616672033>
- Russell, S., Stocker, R., Cockshott, Z., Mason, S., Knight, J., Hanratty, B., Preston, N., 2025. Use of a digital application to enhance communication and triage between care homes and national health service community services in the United Kingdom: a qualitative evaluation. *BMC Geriatrics* 25, 875. <https://doi.org/10.1186/s12877-025-06217-9>

Module Title: Digital skills and research Methods

Module Code: LCHS4007

Group members names and student number : Thasmiya Tariq (2521422) Jannatul Ferdous (2519627) Mary (2507545)





COMMUNICATION/COLLABORATION TOOLS



WHAT WILL BE DISCUSSED?



EVALUATE HOW MICROSOFT TEAMS IS USED
WITHIN GREENFIELD?

EXPLAIN HOW IT HELPS STAFF
COMMUNICATE ACROSS DIFFERENT
LOCATIONS (E.G., BETWEEN CARERS IN THE
FIELD AND THE MAIN OFFICE)?

IDENTIFY BOTH THE ADVANTAGES AND
CHALLENGES WHEN USING MICROSOFT
TEAMS.

THE USE OF MICROSOFT TEAMS WITHIN GREENFIELD

- 1) Instant messaging allows care staff to instantly message supervisors or colleagues for advice or updates. It can be extremely useful for reserve and non-emergency concerns (e.g., medicine requirements, shift changes), but it can also aid in decision-making and problem-solving.
- 2) Shift handovers and updates: Important information (health changes, incidents, and care plan revisions) can be communicated in writing. It avoids misunderstandings between shifts and provides a clear record of conversation.
- 3) Sharing files: care plans, rotas, policies, and risk assessments can all be safely shared. Staff always have access to the most recent version. Also reduces errors caused by outdated information.
- 4) Phone calls and video conferences: they enable fast team gatherings without requiring staff to travel, which is beneficial for oversight, training, and interdisciplinary conversations, enhancing cooperation among different professions, nurses, and managers.
- 5) Accountability and record keeping updates and messages facilitate safeguarding investigations and inspections. promotes professional communication as well.



ADVANTAGES AND CHALLENGES WHEN USING MICROSOFT TEAMS WITHIN GREENFIELD

Better communications across teams

- ❑ Reaching carers, managers, and office workers fast is made simple by group chats, video calls, and instant messaging. beneficial for interdisciplinary collaboration among managers, social workers, nurses, and care staff.

Improves collaboration and community of care

- ❑ Get immediate notifications about any shifts in care requirements or unexpected events. It's simpler to raise issues and quicker to decide on actions. When used in conjunction with a care management system, it helps coordinate care efforts.

Lack of digital skills

- ❑ Some staff may have limited confidence with using technology. Also, staff may need training support, some staff may feel that teams is very overwhelming.

Relaying on technology

- ❑ Sometimes technology can cause problems with communication, like when the signal is bad or an app stops working. It's also not the best choice when you have an emergency.

Confidentiality and data protection risk

- ❑ If employees aren't properly trained, sensitive stuff might get shared by mistake. You really need strong rules to stick to GDPR and keep everyone safe.

Information overload

- ❑ Having too many channels or messages can make it easy to overlook important updates. If you don't manage your notifications well, they can really interrupt what you're doing.



REFERENCE PAGE

- National Health service (2017). *Working in Social Care*. [online] Health Careers. Available at: <https://www.healthcareers.nhs.uk/working-health/working-social-care> (accessed 1st February 2026).

Digital Safety Action Plan

Introduction

Digital strategies have been formally recognized as a critical health systems strengthening strategy to help meet the Sustainable Development Goals and universal health coverage targets.(1) Taking this larger strategy to a smaller health care setting, using the centralized Microsoft 365 tools we have designed a digital safety action plan.

At the very beginning of working out the digital safety action plan, we first looked at the company, clients and nature of their work. We identified that the business dealt with vulnerable people and handled their medical data.

From this, we deduced four main goals for improvement:



Secure
Awareness

Email
Awareness

Data
Management

Confidentiality
and Compliance



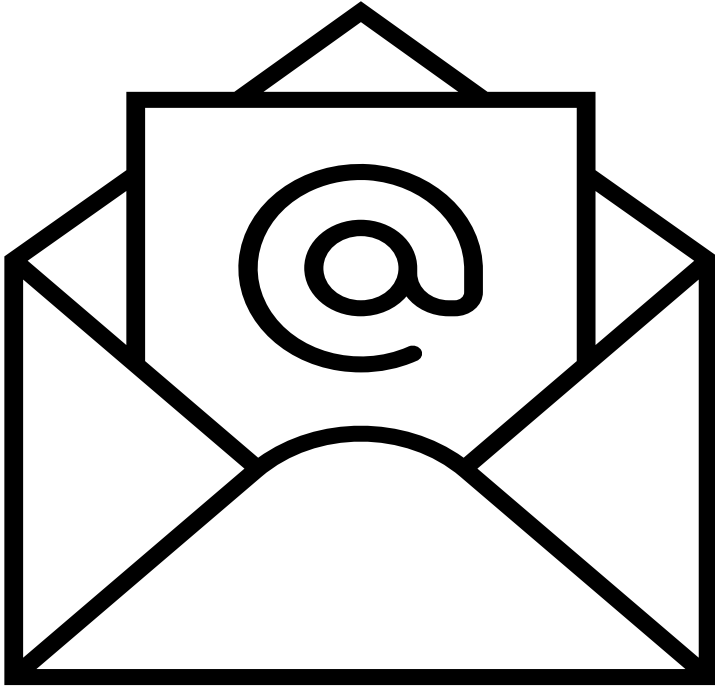
Secure Awareness

Client information held by administration needs to be stored on Sharepoint or OneDrive, on business devices only.

To ensure that staff have secure awareness, effective training will need to be given on all the Microsoft 365 applications. This is an all-round training that gives staff the knowledge and confidence to apply it to their everyday role and to support colleagues in keeping a secure environment.

These mandates, policies, and standards establish a measurable, minimum baseline. The hope is that compliance with these training requirements will result in long-term positive impacts on security behaviours. (3)

Email Awareness



Even with strong cyber security policies an organization can still be hacked because of a human error. Even if people are aware of the policies and their importance they might not behave accordingly. [4]

The main risks staff need to be alert to is phishing, sender verification, and malware in the form of links/attachment. As this can cause serious data breaches, thorough training needs to be given to all new staff before they are given clearance to use this platform.

Recognising suspicious activity, acting with caution and always flagging/reporting any suspicious activity is critical in maintaining digital safety. Using exclusively Outlook for email communication, staff should report this using the report phishing button found within the app.

Data Management

How data is handled and stored is key in understanding any gaps in security. Every piece of data/information handled should only be by the relevant staff member who is trained and cleared to do so. In recent years, the evolving healthcare landscape has underscored the need for nurses to navigate complex challenges such as patient privacy, data security, and regulatory compliance, are crucial for safeguarding patient information and maintaining trust and integrity within healthcare settings.(2)

We will implement a multifactor authentication system to improve security. Also, stronger requirements for passwords - 10 character minimum with no number sequences - and an automatic lock screen when not in use.

Care Co-ordinators and Visiting Carers

- Care Plans

Nurses

- Medical Records

Administrative Staff

- Finance
- HR/Staff records
- Patient details (non-medical)

Confidentiality and Compliance

Applying sensitivity labels on documents and emails ensures it is handled/viewed with the appropriate discretion. The categories selected should be 'Confidential' or 'Highly Confidential' as appropriate.

Using internal communication via Teams and Outlook only.

1 Alain Labrique, Lavanya Vasudevan, Garrett Mehl, Ellen Rosskam and Adnan A. Hyder
Global Health: Science and Practice October 2018, 6(Supplement 1):S1-S4; <https://doi.org/10.9745/GHSP-D-18-00342>

https://www.ghspjournal.org/content/6/Supplement_1/S1.full

2 Ten Ham-Baloyi W. (2022). Nurses' roles in changing practice through implementing best practices: A systematic review. Health SA = SA Gesondheid, 27, 1776. 10.4102/hsag.v27i0.1776

<https://pubmed.ncbi.nlm.nih.gov/35747507/>

(3) Ten Ham-Baloyi W. Nurses' roles in changing practice through implementing best practices: A systematic review. Health SA. 2022 May 25;27:1776. doi: 10.4102/hsag.v27i0.1776. PMID: 35747507; PMCID: PMC9210184.

[4]

Khalid Adnan Alissa, Hanan Abdullah Alshehri, Shahad Abdulaziz Dahdouh, Basstaa Mohammad Alsubaie, Afnan Mohammed Alghamdi, Abdulrahman Alharby, and Norah Ahmed Almubairik. 2018. An instrument to measure human behavior toward cyber security policies. In Proceedings of the 21st Saudi Computer Society National Computer Conference (NCC'18). IEEE, Los Alamitos, CA, 1–6.

<https://ieeexplore.ieee.org/abstract/document/8592978>