ipc
institute of
public care

Driving improvement and innovation in care

Adult Social Care Data and Cyber Security Programme

Final Report Executive Summary

May 2019

OXFORD
BROOKES
UNIVERSITY

http://ipc.brookes.ac.uk

Local Government Association

The Care Provider ALLIANCE

Department
of Health &
Social Care

Adult Social Care Data and Cyber Security Programme

Executive Summary

The aim of the data and cyber security programme is to explore how the adult social care provider sector uses technology and to identify data and cyber security risks faced by the sector as well as to assess the effectiveness of existing support for providers.

The research took place from October 2018 to March 2019 in three local authority areas with a representative sample of 70 care providers. A third of which were care homes, a third homecare services, and a third supported living or ‘other’ services such as day services, respite services, shared lives, and low-level, preventative unregulated services.

How Digital is the Sector?

All providers used information technology to some degree. Information technology use ranged from a single computer used by a small organisation to on-line proprietary care planning systems with all members of staff inputting data via mobile devices. To illustrate and summarise our findings we created three organisational personas to represent the organisations that participated in the research:

1. Type one organisations mostly use paper-based systems. Whilst organisations of this type may vary from those that hardly use any digital systems to those that make regular use of generic systems such as the Microsoft Office Suite, they are unlikely to use care planning software or other sector specific systems and rely on hard copy record keeping.
2. Type two organisations use a mixture of digital and paper-based systems. They are likely to make extensive use of email and generic systems. They may use care planning software or other sector specific systems, however, only more senior or admin staff have their own login to systems or own organisational email address.
3. Type three organisations mostly use digital systems. They are likely to rely on care planning software and/or other sector specific systems as well as email or generic systems. Front-line / care or support workers will have their own login to these systems and are likely to have their own organisational email address.

There was an even spread of organisational personas with, roughly, a third of participating services in each persona type. Geography did not make a difference to a service’s level of digital use, however, organisational size and service type does. Larger organisations are much more likely to make greater use of information technology and digital systems. This is particularly the case for care homes. Small, single site care homes are predominantly persona type one organisations. Homecare services were more likely to be type three personas because of the more frequent changes to documentation and record keeping needed. Organisations with more static recording requirements like supported living, shared lives or unregulated services are more likely to be type two organisations.

Twenty percent of services reported that they use their fax machine regularly, and they are reliant on it to e.g. fax repeat prescriptions to their local pharmacy. This was especially, but not exclusively, an issue for care homes registered to provide care for older people.

Data and Cyber Security Risks

We developed an adult social care provider risk categorisation model that was based upon National Cyber Security Centre guidance. Nine risk categories were RAG rated (red/amber/green/not applicable) for preventative measures and by how ready and able a service would be able to cope for 48 hours without key systems if a problem did occur. We judged that, overall, two thirds of services were rated Green, a quarter were Amber and 7% Red. Ratings varied by persona type as illustrated in the table below.

Overall risk rating	Persona One	Persona Two	Persona Three	All services
Green Amber Red	43% 43% 14%	83% 17% -	71% 19% 10%	66% 27% 7%

We did not come across any instances of services using desktop or laptop operating systems that are no longer supported, e.g. Windows XP, and we do not have any major concerns about providers' ability to keep working if they lost their critical systems. However, a significant minority of services are using Windows 7, which Microsoft have announced it will no longer provide security updates or support for after January 14, 2020. So, there is a potential increased risk to the sector after this date and/or additional costs to keep software up to date. Information flow from the NHS to provider services was also reported as a risk. The greatest cyber security risks were judged to be:

1. Logins and passwords - 30% of services were rated Green.
2. Smartphone security - 40% of services (if applicable) were rated Green.
3. Backups - three quarters of services were rated as Green for their backup arrangements (and 13% rated Red) with a clear link between good practice and services' greater reliance on digital systems.

Existing National Support Materials

There is little awareness of the generic National Cyber Security Centre Guidance or the sector specific Information Governance materials published by the Care Provider Alliance. None of the services were aware of or were using the e-Learning for Healthcare Data Security Awareness programme.

Nearly half of services were aware of the Data Security and Protection Toolkit (DSPT), 29% had heard of the toolkit but had not registered or attempted to complete it whilst 20% had registered and/or completed it to some degree. All providers reported difficulties registering or completing the toolkit.

Recommendations for National Bodies

1. Reinforce across national organisations, and with local commissioners and providers, the Data Security and Protection Toolkit as the single mechanism for use by adult social care providers to self-assess their data and cyber security.
2. Review the content and improve the usability of the Data Security and Protection Toolkit with respect to social care provider completion and continue to not make toolkit completion mandatory for social care organisations that are not operating through the NHS contract at least until this is done.
3. The Care Quality Commission to explore how the Data Security and Protection Toolkit can be incorporated as part of the evidence inspectors use to make assessments of social care providers.
4. Review the existing National Cyber Security Centre guidance on IT security, mobile working and passwords. These should then be promoted by relevant sector bodies to support adult social care providers.
5. The Care Quality Commission to clarify that they do not require paper records to be kept to aid their inspections, and to provide appropriate support to inspectors to apply this policy consistently.
6. Develop new or clarify existing guidance so that there is one agreed and consistent message to the sector on record retention and disposal practice. Guidance should cover records held electronically as well as physically.
7. Propose a practical approach for adult social care providers to undertake due diligence checks on any outsourced IT function to ensure data and cyber security compliance and assurance. This could be through the Data Security and Protection Toolkit.
8. Agree the position across the health and social care system on what constitutes valid evidence of consent in a digital age. Once this position has been agreed, for national partners to promote and advise of this position to respective health and social care organisations.

Recommendations for the NHS

9. Further enable the flow of and access to information from health to social care providers (and vice versa) safely and securely. This should be explored and developed as part of the Local Health and Care Record Exemplar Programme.
10. Support NHS organisations currently relying on fax for interaction with adult social care providers to use alternative digital channels such as secure email.

Recommendations for Local Commissioners

11. Councils to consider supporting local care providers with provision of data and cyber security information, advice and guidance and/or services, which could be on a charged for basis. This support could include data and cyber security training and signposting ‘packs’ for small or local services that are entering or new to the market.
12. Councils to consider extending local contract management arrangements that already take place with providers so that they include an emphasis on safe and secure handling of information.

13. Councils and CCGs to encourage their local care provider markets to comply with recommendation 1, i.e. to complete the Data Security and Protection Toolkit, and consider including this as part of local contractual arrangements and practice.

Recommendations for Service Providers

14. Subject to the recommended improvements to the Data Security and Protection Toolkit (see recommendation 2), care providers should complete the toolkit to self-assess their data and cyber security. In the meantime, care providers should check their organisation's IT security against the National Cyber Security Centre's guidance.
15. Care providers to review password and smartphone security practice against the National Cyber Security Centre's guidance (and where possible consider multi-factor or two factor authentication).
16. Care providers to support staff and volunteers to maintain awareness of data and cyber security risks and good practice through induction training and ongoing awareness raising.
17. Where IT support is outsourced to external organisations, undertake data and cyber security due diligence checks to ensure compliance with national guidance (as per recommendation 7).
18. Care providers to ensure that they have access to a secure electronic data transfer method. Where secure email (other than NHS mail) is in use, register this using the secure email accreditation process so that this is recognised by other care and health professionals and to further support the sharing of information.
19. Care providers to review their business continuity plan to ensure it extends to information technology and digital systems, and test this at least annually.