ipc
institute of
public care

Driving improvement and innovation in care

Adult Social Care Data and Cyber Security Programme

Final Report

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

Contents

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	43%	83%	71%	66%
Amber	43%	17%	19%	27%
Red	14%	-	10%	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.

.

Adult Social Care Data and Cyber Security Programme

1 Introduction

As we use more technology in care services, both to support care delivery and to improve digital connectivity with partner organisations, it is vital that people's information is kept secure, and that the systems we use are reliable. Funding was allocated from the National Cyber Security Programme to commission a programme to conduct on-site research and to support the adult social care provider sector to manage the business risks associated with data and cyber security.

The Local Government Association (LGA), Care Provider Alliance (CPA) and Department of Health and Social Care asked the Institute of Public Care (IPC) at Oxford Brookes University to undertake the adult social care data and cyber security discovery programme. The aims of the discovery programme are to:

- Explore how the adult social care provider sector is using technology, and identify the common and current data and cyber security risks faced by the sector
- Assess the effectiveness of existing support for adult social care providers
- Produce recommendations to support the sector to minimise identified risks

The research took place from October 2018 until March 2019 in three local authority areas: North Yorkshire (NY), Central Bedfordshire (CB) and the Royal Borough of Greenwich (RBG). A representative sample of care providers operating in these areas was asked to take part. Seventy provider services volunteered, which included some services whose registered office is in a different local authority area.

Each participating service received a visit from IPC to find out how the service uses data and technology and received follow up support to help them with their data and cyber security. The areas of investigation for the initial 'discovery' visits covered:

- How personal and sensitive information is received, stored and shared
- Use of data and technology, including cyber security measures
- Staff and / or volunteer logins and passwords
- Staff and / or volunteer training related to data protection and information security
- Business continuity planning and risk mitigation
- The 'reach' and effectiveness of existing data and cyber security national support materials, including the Data Security and Protection Toolkit and the Cyber Essentials Scheme

1.1 Programme Participation

The adult social care sector is very diverse with more than 21,000 independent organisations in England, ranging from big corporate chains to small family-run businesses, charities and social enterprises as well as provision by local authority adult social services departments. These organisations provide an estimated 41,000 adult social care services (Skills for Care 2018 The size and structure of the adult social care sector and workforce in England) of which 40% are Care Quality Commission (CQC) regulated residential services (including care homes and shared lives services), 9% are non-CQC regulated residential services (e.g. homeless shelters, women's refuges), 22% are CQC regulated non-residential services such as homecare and supported living services whilst 29% offer non regulated services, including day services and a wide range of community support and outreach services for vulnerable people.

The programme sought to recruit a group of services which would be as representative of the sector as a whole as possible. However, identifying from the CQC website how many services of a particular type are registered is not entirely straightforward. There isn't a straightforward or consistent way of identifying and listing all of the services which actually operate in an area.

The recruitment of providers to the programme proved to be more difficult than had been anticipated. Initially, letters were sent to a group of providers that had been carefully selected to form a good cross section of the sector. There was, however, a very slow initial response, and further efforts were needed throughout the programme. These included additional mailings, publicity and encouragement by the three local authorities, and direct contact with individual providers. Data and cyber security is a difficult topic with which to interest busy adult social care providers.

Of the three local authority areas, North Yorkshire is by far the largest, and has almost twice as many registered services as Central Bedfordshire and Greenwich combined. We aimed to recruit 33 services in North Yorkshire, and 21 in each of Central Bedfordshire and Greenwich. This represented 1 in 12 regulated services in North Yorkshire, 1 in 6 services in Central Bedfordshire and 1 in 5 services in Greenwich.

In the end, seventy provider services took part. The number of participating services by service type is shown in the table below. Approximately a third were care homes, a third homecare services, nearly a fifth 'other' services, and the rest supported living services. 'Other services' included day services, respite services, shared lives, and unregulated preventative services.

Figure 1: The number of services taking part in the programme by service type

Local authority area	Total	Care homes	Homecare	Supported living	Other services
NY	**34** (49%)	13	10	3	8
CB	**19** (27%)	6	9	2	2
RBG	**17** (24%)	6	4	4	3
Total	**70** (100%)	**25** (36%)	**23** (33%)	**9** (13%)	**13** (18%)

A wide variety of different sized provider services took part in the programme, including small local organisations with less than ten members of staff and services that are part of larger national groups, including five that that are part of the CQC Market Oversight Regime. In terms of funding mechanisms, there was a mix of provider services i.e. those that have mostly private or self-funded clients, mixed funding streams and those whose clients are all public sector funded. There was a similarly diverse range of ownership including private, public and third sector organisations.

The three local authority areas were selected because each was a different type of area with a different type of council. The overall composition of services across the three areas taken together is broadly similar to the overall composition nationally. In relation to the 70 participating services, residential homes and homecare services were slightly under-represented; nursing homes were slightly over represented; and supported living services were over-represented. There were also few services specifically for people with mental health issues. Nonetheless we are satisfied that the group of participating services are representative of the sector as a whole.

2 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 for sending and receiving emails and printing documentation to on-line proprietary care planning systems with all members of staff inputting data via mobile devices. Many organisations use a mixture of paper and electronic systems and have hard copy client files that mirror digital ones.

To illustrate and summarise our findings we created three organisational personas to represent the organisations that participated in the research. This was based on the premise that organisations with different configurations can be grouped together based on how they use data and technology. The behaviours and attitudes of organisations will affect how they use data and technology. The fictitious personas below are descriptions of different types of organisations, based on our research. The aim is to give a more human face to anonymised and abstract information. In particular, they are useful for creating a shared, consistent understanding of types of organisations.

It should be noted that personas are not based on any one organisation, they are an aggregation of our research information. Neither are the personas reflective of sub sectors of the market i.e. it does not matter whether the organisational scenario is a care home or supported living service, for example, what matters is the common behaviours and arrangements in place for data and cyber security. For each persona, two organisational scenarios are given as illustration as well as common behaviours/arrangements and common data and cyber security challenges. Also, to note, some of the challenges will be common to more than one persona. We have tried to capture, across personas, some of the key data and cyber security risks we found.

Organisational persona type one – mostly paper-based systems

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.

Scenario 1A	Scenario 1B
▪ Brilliant Care is a small local homecare agency in a rural location.	▪ Clarence House is a council owned and run care home and day service.

■ An external IT company helped to set up the office IT equipment – one laptop and one desktop computer - and IT security arrangements such as anti-virus software. The computers are backed up using memory sticks, with a prompt to back up every day, but it is hard to remember to do so or make the time in a busy office. ■ Care staff are expected to use their own phones to make and receive calls and texts, to be in contact with the office. ■ If a referral is from the council, the person's details will be sent to us by the council's secure email system. ■ Assessments and care plans are hand written on templates and then typed up in Microsoft Word (printed for signature) and saved on the manager's computer and in hard copy form. ■ Hard copies of client documents are kept in the client's file, which is stored in a locked cupboard in the office, and a copy in the person's file in their home. ■ Daily logs are written by hand by care workers in the person's file in their home. ■ Medication Administration Record (MAR) charts are pre-printed by pharmacies and completed by hand. MAR charts and daily logs are brought back to the office base monthly by care workers. ■ There is a hard copy file for each member of staff with their personal details, references, sick notes etc. Staff complete weekly, hand written timesheets. ■ Timesheet information is transferred onto a password protected spreadsheet for payroll purposes and sent by email to the payroll company who compile payslips. These are delivered by hand back to us and handed to staff.	■ All hardware and software is procured, managed and supported by the council's central ICT Department. Senior and admin staff have virtual desktops on the council's network. There is one 'office' smart phone that senior staff can use when undertaking pre-admission assessments i.e. when they are away from the home. ■ If a referral is internal from the council, the manager will be given the person's unique identifying number and can look up their details on the council's care management system. ■ Assessments and care plans are hand written on templates and then typed up in Microsoft Word (printed for signature) and saved on the network and in hard copy form. ■ Hard copies of client care planning documents are kept in the resident's file, which is stored in a locked cupboard in the office. ■ Hard copy daily care records are hand written and kept in the resident's files. When people's files get too full, old care records are archived in the storage room. ■ Shift handover meetings are held daily and a communication book, with hand written entries, is used if there is significant news. ■ MAR charts are pre-printed by pharmacies and completed by hand. All medicines are kept in a locked drugs cupboard, to which only senior staff only have access, and are audited and checked off. ■ The home manager can access the council's online staff portal to view staff details and training records. ■ Staff are salaried and do not have to complete timesheets. However, if they work extra shifts then the manager can enter/audit timesheets to authorise additional payments.

Behaviours/arrangements

- The manager is in constant contact with care workers by phone and text or in person: *"we know our clients well and for confidentiality use only their initials in any emails or texts".*
- The weekly care home rota is printed out and displayed in the staff room, changes are marked on by hand.
- The homecare agency roster is printed out and left in care staff pigeon holes in the office, changes are communicated by phone or text.

Data and cyber security challenges

- For community-based services, transporting hard copy personal and sensitive data back and forth between clients' homes and the office is a data security risk.
- Mobile phone signal coverage is poor in the local area and sometimes the manager can't contact staff if they are away from the office/home.
- Although the service has the client's consent to share medical data, it is often not told about changes to their medication, particularly on hospital discharge. Some GPs and pharmacies are much better than others at seeing the implications and liaising with the service.
- The Warfarin clinic won't email the care home its international normalised ratio (INR) results. The council does not allow services to use fax so the home has to send someone to collect them from the clinic.
- The homecare agency recognises that moving away from paper copies for clients' files would cause some anxiety but thinks that it is stopping the business expanding.

What they might say

"We probably ought to use more IT, but paper works well for us"

Organisational persona type two – a mix of paper and digital systems

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 such as the Microsoft Office Suite. 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.

Scenario 2A	Scenario 2B
■ Somewhere Community and Voluntary Support provides non regulated, early intervention, preventative support and advice services.	■ St Stephen's is a medium sized, regional group of care services, including a supported living service. ■ An internal IT Department is based in the Head Office, which sets up and

■ One of the senior management team is good with computers and looks after the IT arrangements, supported by the online system provider if needed. ■ There are employed staff and the service relies significantly on volunteers as well, who are expected to use their own phones to be in contact with the offices. ■ An online propriety software system is used to record staff and volunteers' data and basic client details as well as billing information. ■ There is an electronic record for each member of staff and volunteer with their personal details, references, sick notes etc. ■ The on-line system has access control on log in so that only line managers can see staff details. ■ Work is scheduled using the online system and rosters/details can be mass emailed (bcc'd) to support workers and volunteers from the system.	oversees the IT arrangements in all the services. ■ Senior and office staff have desktop computers and/or laptops and smart phones. Support workers will use their own mobile phones to receive text messages and phone calls and their own devices to access emails sent to their personal accounts. ■ An online propriety software system is used to record staff details and basic client details as well as billing information and scheduling. ■ If a supported living referral is from the council, the person's data will be sent by a secure email system. ■ Hand written assessments and plans are typed up in Microsoft Word and saved on the network. An electronic folder is created for each person and accessed remotely via a virtual private network. ■ There is a hard copy folder for each client held in the office and one in the client's house. ■ A monthly, password protected, roster is emailed to support workers and a weekly update if it changes.

Behaviours/arrangements

- There are some shared on-line system logins by role.
- The Locality Manager runs an end of month report for finance to reconcile activity with payroll.
- Staff are sent their payslips, which are password protected, by email to their personal email address.

Data and cyber security challenges

- The cost of keeping IT equipment up to date: "*we know we need to upgrade several machines to Windows 10 and one of our offices has very poor broadband connection speeds*".
- Ensuring that the email system is a secure one.
- Front line staff (and volunteers) are focussed on providing good support and it's hard to get them to realise the importance of data and cyber security. They have variable skill levels, and some have never used a computer before.

- The on-line system is quite new – less than two years old – the service hasn't yet had to think about archiving or disposing of old records.
- Undertaking due diligence on the third party proprietary IT system suppliers that handle personal and sensitive data.
- Different funding organisations ask for different GDPR compliance information in tenders e.g. Cyber Essentials or ISO 27000 information security standards.

What they might say

"They [our online system provider] are the IT experts, that's why we bought their system in the first place. I assume that they are GDPR compliant and everything is backed up in the cloud somewhere"

Organisational persona type three – mostly digital systems

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 such as the Microsoft Office Suite. Front-line / care or support workers will have their own login to these systems and are likely to have their own organisational email address.

Scenario 3A	**Scenario 3B**
■ The Laurels care home is part of a large, regional group of care services. ■ It has Wi-Fi for residents and visitors to access as well as staff. ■ The group's internal IT Department oversees the IT set-up and security arrangements, such as anti-virus software, for all homes in the group. ■ A propriety software system is used for all staff data, including payroll, the home's rota and billing/invoicing, and another system is used for care planning. The systems don't interact or populate each other. ■ The care plan is typed into the client record system and printed for signature. Hard copies of signed documents are scanned and saved to the system then securely shredded. Office staff scan and save all assessments, consent forms, plans, letters, DOLS etc into the care planning system. ■ Daily logs are entered directly into the care planning system by care staff	■ Handy Care is a small local homecare agency that operates in a metropolitan area. ■ An external IT company helped to set up the office IT equipment –laptops for all office-based staff - and IT security arrangements such as anti-virus software. ■ A propriety software system is used for electronic call monitoring, and another system is used for rostering and care planning. ■ Care staff are given an allowance to use their own phones for work. They are expected to download the electronic care monitoring and care planning system Apps and to use WhatsApp to be in contact with the office. Staff can see the roster on their phones along with key client details of those they visit that day. ■ Assessments and care plans are typed in a Google form (printed for signature) and then scanned and saved to the care planning system and the hard copy securely shredded.

using mobile devices provided by the organisation. ▪ An eMAR system is used for medication. The eMAR and care planning systems are meant to cross reference but don't. Separate log ins are needed by staff. ▪ The home has access to a two-way video link to health professionals – clinicians can see, and talk to, residents and care home staff to enable virtual assessment and prescribing.	▪ Hard copies of client documents are kept in the client's file in the person's home. ▪ Care workers make daily notes in the care planning system App and a What's App groups is used to communicate with and between staff. ▪ MAR charts are pre-printed by pharmacies and completed by hand. MAR charts and daily logs are brought back to the office base monthly by care workers.
Behaviours/arrangements ▪ All front-line / care or support workers as well as office staff and managers have their own organisational email address and login to the system(s). ▪ The service has 'made the leap' and provided smart phones/tablets/laptops (or a phone allowance) for all staff. ▪ The service is planning to roll out further modules of the care planning system so that clients or their family as appropriate can remotely access their own records. ▪ The service is confident that their online systems will always be available to them.	
Data and cyber security challenges ▪ The local pharmacy will only accept repeat prescriptions by fax. ▪ The service wants to be allowed to access the NHS system to be able to see health records for their clients. ▪ The cost of providing mobile devices to all staff and/or working out how to lock down and properly control staff's own mobile phones with a 'Bring Your Own Device' policy. ▪ The service worries that their CQC inspector will insist on seeing hard copy files. ▪ Staff have multiple system login passwords to remember, with system forced password changes every six weeks.	
What they might say *"Our CEO has a vision of the organisation as paperless in the future"*	

We categorised participating provider services into the organisational personas outlined above. The number and proportion of each service type categorised by organisational persona type is shown in Figure 2 below. There was an even spread of organisational personas with, roughly, a third of participating services in each persona type.

Figure 2: The number and proportion of services in each organisational persona

Service type	persona type one	two	three	Total
Homecare	**4** (18%)	**8** (35%)	**11** (48%)	**23** (100%)
Care homes	**13** (52%)	**3** (12%)	**9** (36%)	**25** (100%)
Supported living	**2** (22%)	**6** (67%)	**1** (11%)	**9** (100%)
Other	**4** (31%)	**8** (61%)	**1** (8%)	**13** (100%)
Total	**23**	**25**	**22**	**70**

A third of services mostly use paper-based systems. Of these 23 services, 19 are small, local organisations, 2 are local authority provided services, and 2 are small services that are part of a larger, national group. Of the 13 persona type one care homes, 10 are single-site homes and 2 are local authority provided homes. All the homecare and supported living services that mostly use paper-based systems are small, local organisations.

A third of services use a mixture of paper and digital systems. There are few care homes in this category and a high proportion of supported living services; two thirds of supported living services use a mixture of paper and digital systems.

A third of services mostly use digital systems, including nearly half of the homecare services. All the homecare organisations of this type are small or medium sized services and many of them are relatively new organisations that have been set up with a greater use of information technology from the beginning. In this persona type, 6 out of the 9 care homes are part of larger regional or national groups.

Geography did not make a difference to a service's level of digital use, however, organisational size and service type does. Perhaps unsurprisingly, larger regional or national organisations are much more likely to make greater use of information technology and digital systems.

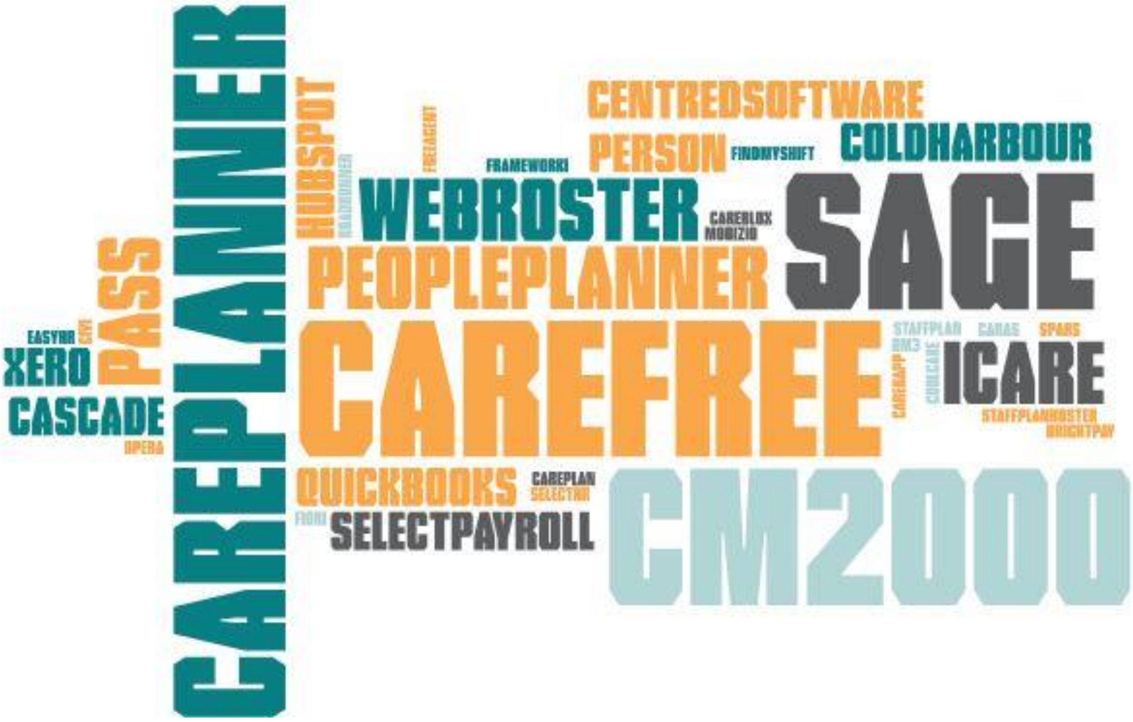
This is particularly the case for care homes. Small, single site care homes are predominantly persona type one organisations with 10 out of 13 small homes using mostly paper-based systems. Care homes tended to fall into one of two camps: they were type one personas reliant on paper-based systems or they had 'gone digital' and were making extensive use of proprietary care planning systems to record the wealth of data generated about their residents. Residential services like care homes do not have the challenge of community-based care staff using mobile devices to access digital systems and hence their care workers are more likely to have their own login to these systems rather than to be type two organisations.

Non-residential services such as homecare and supported living services as well as some of the 'other' and unregulated services do face the challenge of community-based care staff accessing digital systems. Homecare services were more likely to be type three personas because of the dynamic nature of the care and support given, the faster 'churn' of people who use their services and the more frequent changes to documentation and record keeping needed. Organisations with more static recording requirements like supported living or shared lives services are more likely to be type two organisations. This is also the case for, for example, unregulated services if there isn’t the need for detailed recording of care information by front line staff or volunteers.

No providers were entirely ‘paperless organisations’ although some kept no permanent hard copy personal or sensitive staff and / or client data. A few have ambitions for their records to become wholly digital. The barriers to this were stated to be a) the investment cost b) lack of appropriate software for some parts of their operational process c) nervousness about keeping no client hard copy records and d) demands by other organisations for them to retain paper records or use faxes. For instance, it was reported that one local authority requires there to be paper copies of all client documentation available. CQC inspection practice, or providers’ perception of that practice, is a barrier to greater use of digital in the sector. We were told by some services that CQC inspectors insist paper files are kept because it makes their checking process easier.

As well as generic systems such as the Microsoft Office Suite, a wide variety of specialist proprietary software was used in services such as PeoplePlanner, CareFree, CM2000, iCare, CarePlanner, SAGE, Cascade, Hubspot, Person-centred Software, the PASSsystem, Civi etc. Many providers access these systems on-line, hosted in the cloud by the software company. Whilst these services had, usually, asked for e.g. guarantees from the hosting companies of downtime and backup arrangements, the majority had not undertaken GDPR due diligence of cloud contracts for their storage containing personal confidential data. In many instances services were not aware of the requirement or did not understand how to verify the security provisions operated by hosting companies*.* A minority of providers had attempted to undertake due diligence but had not been satisfied with the answers they had been given. One commented that *“The relatively small size of our organisation means it is difficult to request or stipulate custom requirements with suppliers.”*

Figure 3: Specialist software systems used by participating services



What struck us is the number of organisations that have recently, or are about to, change their systems. Many of the organisations visited recently have or are considering purchasing new systems or have plans to extend the use of their existing systems.

2.1 Use of Fax

After the programme start, we were specifically asked to find out the extent to which services have and use fax machines. Just over a third of provider services have a fax machine (36%), however, just under half of these either don't use or very rarely use their fax machine. One provider that was part of a large group of services for people with a learning disability commented that "*a part of the old CQC regulations [was that] a fax machine was required to be present in our homes, however, we are currently phasing them out of services*".

Figure 4: The number and proportion of services that have a fax machine

Have a fax machine?	Number of services	Proportion of services
No	38	54%
Yes, but rarely used and not reliant on it	11	16%
Yes, used regularly and reliant on it	14	20%
Not known	7	10%

The remaining 14 providers – which is 20% of the total 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. For all but two of these services the continued use of fax machines was reported not to be a choice that services had made but a practice that was forced upon them by NHS organisations or, to a lesser extent, by local authorities. Providers were not happy with the arrangements but had not been able to persuade partner organisations to change their ways and would welcome any support from local or national commissioners to influence the policy of NHS organisations in particular. Comments included:

"*Our local pharmacy will not accept scanned and emailed prescriptions. They will only accept a fax.*"

"We receive faxed discharge letters as hospitals will only fax info and not use email (even if documents are password protected). Similarly, sometimes we have to request prescriptions form GPs by fax as they are reluctant to use email. We have little sway with the NHS to persuade them otherwise."

"We are reliant on it to receive INR blood results by fax"

"Warfarin info for clients and some GPs ask us to fax them medication details - they won't talk to us until we send them a fax. We would like not to have to use it as we don't feel it is secure but some health service people insist on it."

"Our local Drs surgery insists on faxed list of residents and won't accept other methods."

"It's used for brokerage/care package changes"

"We receive Continuing Healthcare funding and we have to fax our applications for this, we are required to do so. Also, it is sometimes used if we need instant info from a GP as they will only fax to us and don't use email we find (practice nurses will though)".

This was especially, but not exclusively, an issue for care homes registered to provide care for older people.

3 What are the Data and Cyber Security Risks?

Identifying the common and current data and cyber security risks faced by the sector is a key part of this research. We did this in two ways. Firstly, at the conclusion of each provider service initial 'discovery' visit we asked them what they perceived to be their main data and cyber security risks. Secondly, IPC developed a risk categorisation model that we used to generate an overall risk rating. The IPC researcher categorised each service according to (i) how much they use digital applications (persona type one, two or three as described above) and (ii) what data and cyber security preventative measures were taken. An overall risk rating could then be assigned. Services that did not take many preventative measures but had little digital use would clearly be of less concern than the services that had the highest digital use and took few data and cyber security preventative measures.

There are two caveats to this approach to risk categorisation. This was a voluntary research programme and IPC are not inspectors. We could not always test the veracity of the information we were told and we were reliant on the knowledge of the people whom we met with. Some services, for instance, could not provide us with answers to the more technical questions within the timeframe available: some risks were therefore categorised as not known. All risk ratings are the judgement of the IPC researchers, which were made on the information available to us, and not cross checked by the services. Therefore, they should be taken as a rough guide for the sector as a whole and a starting point for the development of a digital maturity risk categorisation system for social care.

The second caveat is that these ratings focus on digital applications and preventative measures. They do not rate existing, non-digital data security risks such transporting hard copy personal and sensitive records between community-based service provider offices and clients' homes for instance.

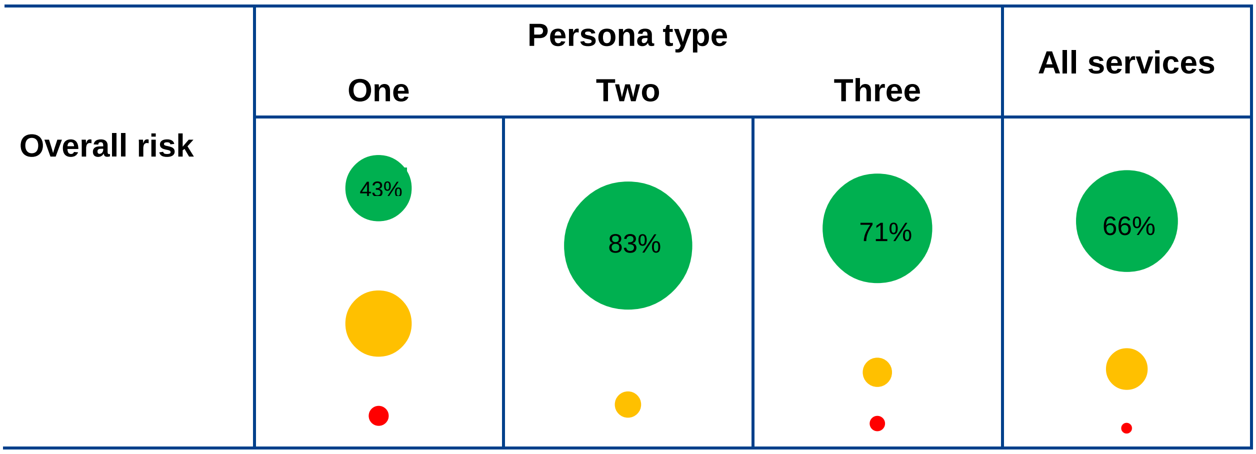
The risk categorisation ratings were based upon the National Cyber Security Centre's Cyber Security: Small Business Guide, which has a useful infographic that gives a summary of low cost, simple techniques that can improve cyber security within all organisations, and 10 Steps to Cyber Security as well as key controls suggested by the Cyber Essentials scheme.

Nine risk categories were RAG rated (red/amber/green/not known or not applicable) for preventative measures – be they technical (e.g. unsupported systems) or people (e.g. lack of training) or process (e.g. default passwords used) - and by how ready and able a service would be able to cope for 48 hours without key systems if a problem did occur. The risk categories are described below:

- IT security - boundary firewalls and malware protection are in place and patch management is supported i.e. IT operating systems are up to date
- Physical security – good security measures for the building(s) where hard copy documents or IT devices are stored and access to personal or sensitive hard copy documents is restricted within the building(s)
- Mobile device security – mobile devices (not phones, see below) that leave the safety of the office (or home) need even more protection than 'desktop' equipment and should be protected by encryption/operating system password/two factor authentication and kept up to date. This may not be applicable to all services
- Smartphone security – smartphones provided by the organisation are protected by PIN/password/fingerprint recognition, can be tracked, locked or wiped if lost or stolen, and the device (and all installed apps) are kept up to date. Alternatively, a ‘bring your own device’ (BYOD) policy implements these precautions for employees’ own phones if used for organisational purposes. This may not be applicable to all services as we discounted phone use for calls and texts
- Backups - regular backups of important data are taken, automatically, to a separate storage facility or to the cloud
- Logins and passwords – do not share system passwords, change all default passwords, avoid using predictable passwords, and do **not** enforce regular password changes
- Policies – data protection, data quality, data security and record keeping policies, or equivalent, are in place and understood
- Staff and/or volunteer education and awareness – maintain awareness of data and cyber security risks and good practice, including mandatory **annual** awareness raising
- Business continuity - would the service be able to cope for 48 hours if a problem occurred with their key systems

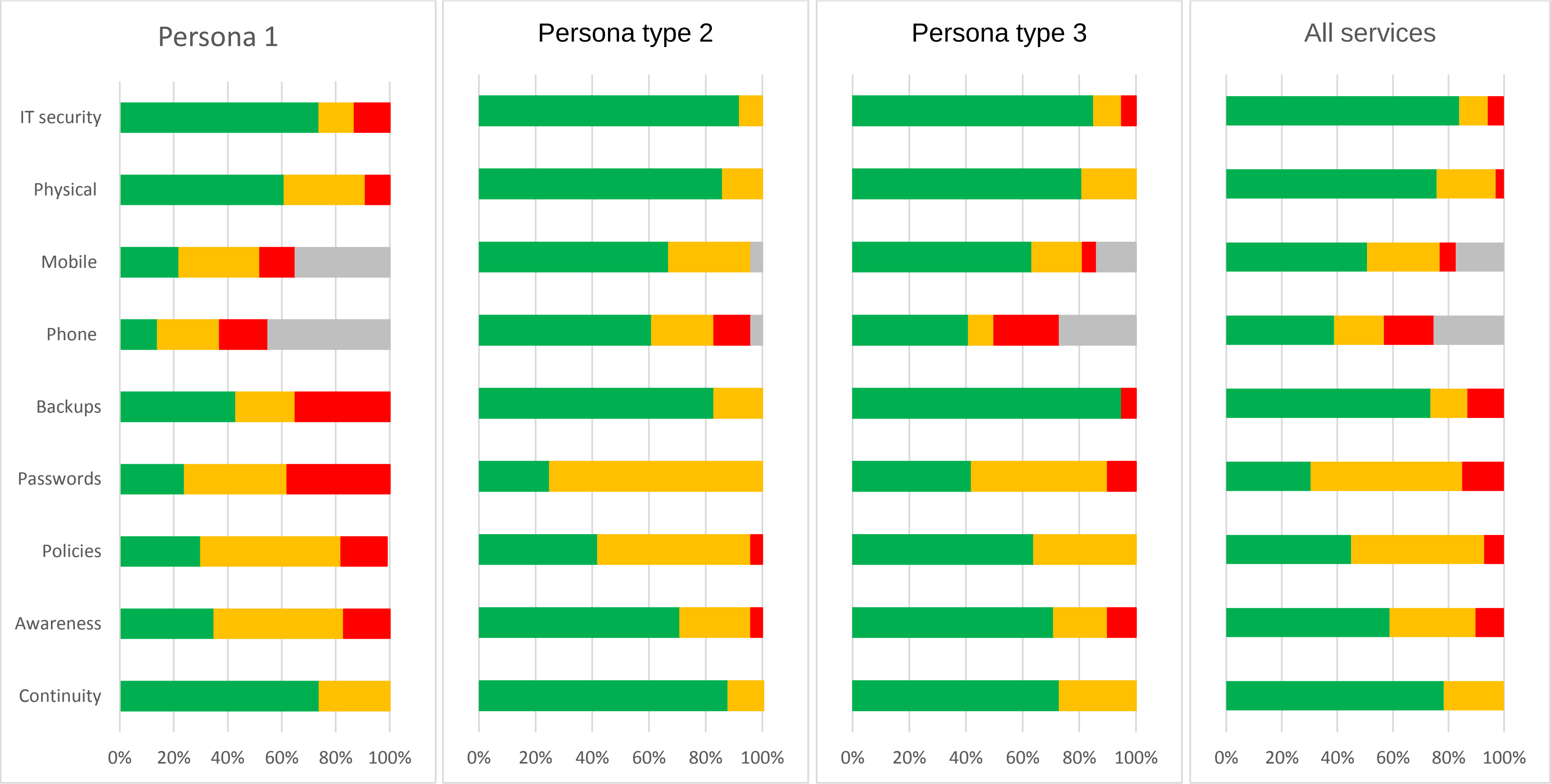
Each risk category was RAG rated as well as an overall risk rating for each persona type. We judged that, overall, two thirds of services were rated Green, just over a quarter were Amber and 7% Red. Ratings varied by persona type as illustrated in Figure 5 below.

Figure 5: The percentage of services categorised as Red, Amber or Green by organisational persona type



The percentage of services categorised as Red, Amber or Green as a proportion of known responses (i.e. discounting not knowns) for each risk category is given in the appendix and illustrated in Figure 6 below.

Figure 6: The percentage of services categorised as Red, Amber or Green for each risk category and by persona type



In terms of IT security, the vast majority providers had done the basics. Most of them have a firewall, have operating system updates (patches) applied, and have antivirus software installed and/or activated. We did not come across any instances of services using desktop or laptop operating systems that are no longer supported e.g. Windows XP. 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.

We rated IT security as Red for 6% of services – for lack of a firewall and/or antivirus software – which was more of an issue for smaller, type one organisations, but these organisations are reliant on paper-based records and this risk is less of a concern for them. Only one digital service was judged to have Red IT security risks.

In terms of specific risks for the sector, overall the greatest risks are:

1. Logins and passwords
2. Smartphone security
3. Backups

3.1 Logins and Passwords

We found the biggest risk in the sector, with only 30% of services being rated Green, was logins and passwords. This is a risk that affects all service types and across all organisational personas. Nearly all organisations relied on senior staff, administration staff and/or care and support workers to login to care planning or work scheduling systems, emails and/or networks or drives on a daily basis. They use passwords or PIN numbers to do so, often without any other technical controls on devices. The issues of concern for this risk category included:

- Not changing default vendor-supplied passwords that come with system, software or hardware purchases.
- A simple default password, e.g. 1234, is set for all new staff who are expected to change it when they first login to the system or device, but the system does not force this and neither is it checked.
- Users are forced to change their passwords regularly, and some staff will have multiple passwords, leading to people writing down their passwords or using an easy to guess formula.
- Passwords are shared between users and/or people use the same passwords at work as they do at home.
- Technical controls are not used to e.g. bar the most common password choices, set minimum length passwords, or to lockout accounts after unsuccessful attempts.
- Password policy is not reinforced with staff training to help users to avoid creating passwords that are easy-to-guess.

3.2 Mobile Device and Smartphone Security

Desktop computers and laptops are commonly used, but there is much less use of tablets and the use of (organisation provided) smartphones is often restricted to senior management or head office / admin staff. Providers are aware of the security risks of laptops - as mobile devices - and take steps to minimise this. For example, a policy of not storing files on the laptop, with laptops used solely to access online systems or a virtual private network (VPN) via a password login. We rated mobile device security as Red for 6% of services (if applicable). Some services had laptops with encrypted storage devices, or two factor authentication was used, but a quarter did not.

That awareness of the importance of additional protection for mobile devices did not always extend to the use of smartphones. We found smartphone security to be the second biggest risk in the sector with only 40% of services (if applicable) being rated Green for their smartphone security. Many services do not view smartphones as mini mobile computers and do not take the same precautions as they do with laptops e.g. up to date systems or apps and antivirus software, apps to track, control or wipe the content of phones if lost, or the ability to restrict use of the phone to specific apps. This is compounded by the number of organisations that do not provide smartphones to all (or any) of their employees (or volunteers) and do not control organisational phone use with a bring your own device (BYOD) policy. BYOD policies, if they exist, are very hard to enforce and services do not actively check that staff implement them. This is a particular concern for type three homecare organisations that do not provide their care workers with smartphones and rely on staff setting a PIN number or using a strong password to login to a care planning app.

3.3 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: type one = 43%; type two = 83% and type 3 = 95%. This was the third biggest risk in the sector overall, but not securely backing up data is more of a risk for type one organisations. These organisations are reliant on paper-based records and this risk is less of a concern for them in terms of the impact it may have. However, fewer services of any type proactively or routinely test their back-ups, with only about a third of services undertaking disaster recovery testing, the rest relying on the fact that *"we've been able to get our data back in the past when we've needed to"* or not ever having considered it at all.

3.4 Other Risks

We do not have any major concerns about providers' ability to keep working if they lost their critical systems. All providers thought that they would be able to operate in the short term if they lost their critical systems, reverting to paper or having arrangements in place for e.g. offline access to eMAR systems. However, we saw little evidence that these plans had been written down and whilst 90% of services have contingency plans, we are not convinced that the scope of these always extends to information technology and digital systems.

When we asked services what they perceived to be their main data and cyber security risks, most responded with "people" or a variation on that theme such as:

- *"People sending out sensitive data accidentally to the wrong people i.e. human error*
- *Hard copy documents being left somewhere they shouldn't*

- *Files are in use by many people, staff go in and out of offices and cupboards can be left open and not locked*
- *Poor IT habits of staff e.g. sharing passwords*
- *We worry about being hacked but more likely is a member of staff leaving paper records somewhere*
- *Hard copy sensitive data is being transported regularly*
- *Awareness by staff of the issue, particularly infrequent users*
- *Staff not necessarily being aware of what data breaches are"*

We would agree that transfer of data of a key risk, whether that is a homecare service regularly transferring sensitive hard copy documents between clients' houses and the office base or sending data by non-secure email. Many provider servicers did not have a secure email system, or did not know if they did, and did not have access to NHSmail.

Other (technological or process) risks identified by services included system outages (particularly if a virtually paperless operation), lack of password protection on emails, and not knowing how long to keep documents and how to properly archive electronic data.

All services are very conscious of the importance of confidentiality, information governance and the data protection principles. For example, most have good physical security in place in buildings that store hard copy personal and sensitive data, and securely shred hard copy files as standard. Data protection training seems to be mandatory – we estimate that 90% of services undertake regular data protection training or awareness training. However, our impression was that did not always extend to cyber security awareness. For some type one organisations that mostly use paper-based systems this is not such an issue. It is important, however, that services that use digital systems ensure that their staff maintain awareness of data and cyber security risks and good practice, including annual awareness raising. This should extend from front line care and support workers to senior management, who can be the worst offenders. In particular, any staff who work away from the office or home should be given training and equipment needed to undertake safe mobile working, for example:

- Encrypted laptops and/or two factor authentication
- Don't connect to unknown Wi-Fi hotspots and instead use 3G or 4G mobile
- Privacy screens on laptops to prevent 'shoulder surfing' if working in public places
- Advice and/or training in password setting

Information flow from the NHS to provider services was also reported as a risk. For example, poor communication from surgeries or pharmacies if their clients' medication changes, or not seeing hospital discharge letters. *"We are often not told about changes to clients' medication and find out from clients or by seeing the medication in their house*. *Some GPs and pharmacies are much better than others at realising the risks of this and liaising with us.*" It was felt that this was due to the policy or attitude of the establishments concerned: *"some GPs won't share medication data with us even if we have consent"*. The issue of poor communication and information sharing is one that was highlighted in CQC reviews of local health and social care systems (CQC 2018 Beyond barriers: How older people move between health and social care in England).

Not being able to access their clients' relevant NHS records or data and not being able to email NHS organisations was identified as a key risk by the sector.

4 How Effective are Existing National Support Materials?

Assessing the effectiveness of existing data and cyber security national support materials for adult social care providers is a key part of this research. In particular we were asked to establish the 'reach' and effectiveness of the Data Security and Protection Toolkit (www.dsptoolkit.nhs.uk/) and the Cyber Essentials Scheme (https://www.cyberessentials.ncsc.gov.uk/), see below.

In general, our impression was that there is little awareness of the generic National Cyber Security Centre Guidance or even the sector specific Information Governance materials published by the Care Provider Alliance. However, for those that were or when made aware of the CPA support materials – as part of this programme - services were uniformly appreciative of the guidance and templates available to assist them to complete the toolkit. Comments included: *"Recommended - very down to earth, easy to understand, good templates. Privacy statement of a sensible size."* Note that since the completion of the fieldwork the Care provider Alliance has published www.digitalsocialcare.co.uk/, which is a dedicated website to provide advice and support to the sector on technology and data protection.

e-Learning for Healthcare (e-LfH) is a Health Education England Programme working in partnership with the NHS and professional bodies to educate and train the health and social care workforce. E-LfH provides a range of online training sessions for NHS and related staff, including a Data Security Awareness Programme that is aligned to the health and social care data security standards and contains an eAssessment. We understand that this training is freely available to social care providers if they have an NMDS-SC or Organisation Data Service (ODS) code. More information is available on the Care Provider Alliance website: https://www.careprovideralliance.org.uk/data-security-training.html. However, that is not clear on the eLfH website itself (https://www.e-lfh.org.uk/programmes/data-security-awareness/) and is therefore likely to be a barrier to social care organisations registering for or using this training. This resource should be promoted as freely available to social care provider services or a social care specific resource should be developed.

None of the participating services were aware of or were using the e-LfH Data Security Awareness programme. This is in contrast to the Information Commissioner's Office (ICO), which most services seemed to be aware of and had used the ICO's support materials to assist them to review compliance with the General Data Protection Regulations (GDPR).

Larger providers who worked with multiple councils gave examples of the differing data and cyber security requirements that they are asked to comply with, such as Cyber Essentials, Cyber Essentials Plus, the Data Security and Protection Toolkit and ISO 2700 standards as well as councils' individual tendering or contracting requirements. This was in addition to the requirement to complete the toolkit if they operate through the NHS Standard Contract. There was a plea for standardisation of requirements from commissioners.

4.1 Data Security and Protection Toolkit

In 2016 the National Data Guardian Dame Fiona Caldicott recommended 10 data security standards for every organisation handling health and social care information. In 2018 the NHS Information Governance Toolkit was updated to reflect GDPR and the 10 standards and re-launched as the Data Security and Protection Toolkit (DSPT).

Social care providers who operate through the NHS Standard Contract needed to comply with the DSPT from April 2018 and complete it by 31st March 2019. The DSPT should be completed once per financial year thereafter. For those who do not operate under an NHS Standard Contract, there was no mandatory action to take in 2018, but it was recommended that services start to comply with the DSPT from April 2018. Completing the toolkit could enable services to access NHSmail, which is a secure email system.

At the start of our engagement with services we asked providers whether they were aware of the DSPT before signing up to the programme. Nearly half of the people who we initially spoke were aware of the toolkit, 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. This figure was significantly higher in Central Bedfordshire where the council had provided training sessions to support providers to understand the toolkit and work through the standards it contains.

Figure 7: The percentage of services that were aware of DSPT by local authority area

Are you aware of the DSPT?	**NY**	**CB**	**RBG**	**Total**
Yes - registered	13%	38%	15%	20%
Yes – but not registered	33%	12%	38%	29%
No	40%	25%	38%	36%
Not sure	13%	25%	8%	17%

Whilst a fifth of providers had registered on the toolkit, few had actually completed it, although some had completed the previous NHS Information Governance Toolkit. We think that only three providers had completed a DSPT assessment prior to the start of the programme.

We sent providers information about the DSPT and encouraged them to register and start the toolkit prior to the discovery day. We asked for feedback of people’s experience of the DSPT. Providers that had previously registered on the NHS Information Governance Toolkit commented that the new toolkit was easier to complete. However, that praise was tempered by continuing usability issues i.e. that improvement was because it was coming from a low starting point of user friendliness.

All providers reported difficulties registering or completing the toolkit. This was not helped by the fact that the look up function for the ODS code was only available to users with access to the HSCN or N3 network during some of the period that the research took place. Many people fall at this first hurdle as (very busy) managers, particularly of small providers, do not have the time to persevere and do not know what an ODS code is. A typical comment on the registration process was *“I found this complicated - had to email Exeter NHS - took a while to get going”.*

Several people commented on the difficulties they had in knowing how to start as the home page (https://www.dsptoolkit.nhs.uk/) is not intuitive. Comments included: *“The initial screen (what's new) is not user friendly and I was not sure what to do when I got there.”* and *“Initially not obvious where to start - needs a summary on the outside which says "CLICK HERE TO START"!!”.*

In addition, people commented on the size of the toolkit and hence the length of time it took to complete. It was perceived as overly complicated, not proportionate to the size and type of organisation. Specific comments included:

“Some parts were useful but some parts worded unhelpfully and not always sure relevant to this type of service.”

“Lack of clarity re meaning in places”

“Clumsy wording and repetitive”

“On the training day I saw a sheet which highlighted non-relevant questions - wish the on-line version showed which ones where not relevant for a care home. So I spent ages trying to find out answers for things that were not relevant to the care home.”

“Overall not hugely useful as content picked up already through GDPR/data protection work - some new things for me - but overall time to complete was long.”

“A very involved process and significant work to produce an Information Asset Register and RoPA but has given further robustness to data management and protection arrangements and staff awareness of the issues.”

“Much better than the old IG toolkit, but still developed for NHS and not social care governance structures of organisations. It is very resource intensive and does not work well for an organisation our size. A lot of the questions are about the organisation's central arrangements and policies, but some, eg Info Asset Register, are home specific and are hard to answer for the group as a whole. It would be much more helpful to have sub-registrations for each home and then home managers can complete their section and that can be tracked locally.”

The toolkit was a key focus for follow up support provided by IPC. Our view, based on providing this support, is that the vast majority of providers, and particularly smaller ones, will struggle to register and complete the DSPT. The registration process is too complicated - the whole system around ODS codes is confusing – and the service request response that providers receive from the helpdesk can be unclear. Services do not understand how and when to use their HQ ODS code (A***) versus one or more of their site ODS codes (V****). In addition, there are no links to the CPA support materials from the toolkit itself, the reduced Entry Level requirements for social care providers is not visible to services until after they have completed the assessments, and in our view the Entry Level requirements do not focus on key assertions.

We would encourage councils and CCGs to support social care providers to register and complete the DSPT by e.g. finding and supplying ODS codes to all local services, and providing workshops, drop in clinics, or a ‘practical completion advice’ phone line as well as helping them to access NHSmail. We understand that NHS Digital has been working with health and care organisations to continue to improve the design of the toolkit and process of completion. We would support additional usability testing being undertaken with adult social care providers as further improvements are made to the toolkit (as per recommendation 2 below).

4.2 Cyber Essentials

Cyber Essentials is a national scheme that helps services guard against the most common cyber threats and demonstrates organisations' commitment to cyber security. Cyber Essentials is a self-certification scheme that is checked by an accredited body. Currently, it costs £300 per year to obtain the certificate. Cyber Essentials Plus, which is quite a bit more expensive (cost will depend on size and set up of the organisation but likely to be a few thousand pounds), is similar but an external body tests your cyber security. It is not a legal requirement to have Cyber Essentials although local authorities or other funders may require, through contracts, that services have Cyber Essentials certification. Having Cyber Essentials Plus prepopulates some of the DSPT assessments but having Cyber Essentials does not. We recommend that Cyber Essentials is recognised by the DSPT in the same way that Cyber Essentials Plus is.

At the start of our engagement with services we asked providers whether they were aware of the Cyber Essentials scheme. Nearly a third of the people who we initially spoke to had heard of the scheme. Although 31% of services were aware of the scheme, in total, only three providers actually had Cyber Essentials accreditation prior to the start of this programme, and one had Cyber Essentials Plus.

Figure 8: The percentage of services that were aware of Cyber Essentials by local authority area

Are you aware of the Cyber Essentials scheme?	NY	CB	RBG	Total
Yes	30%	25%	38%	31%
No	63%	75%	62%	66%
Not sure	7%	-	-	3%

We asked services what was their experience of Cyber Essentials? Most respondents did not have a view as they had not experienced it, but those that did replied:

"85% good but certain things (on the self-assessment) it was not clear what was being asked because of the terminology."

"Viewed as expensive to implement and 'porting' was the main issue the organisation had to deal with to achieve accreditation."

"Was ok - helpful - allows you to take stock/prompts thinking about the various aspects of this area. Lots of questions to be answered! Would be nice to have cyber essentials plus (to have the audit) - maybe next year but cost implication."

"Fine"

5 Recommendations

We propose the following recommendations for national bodies, the NHS, local commissioners and service providers, to support the sector to become as robust as it can in reducing the risk and impact of a potential data breach or cyber security threat.

5.1 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.**

   Context: The report by Dame Fiona Caldicott in 2016 'Review of Data Security, Consent and Opt-Outs' and the Government response in 2017 'Your Data: Better Security, Better Choice, Better Care' highlighted that Government would use the Data Security and Protection Toolkit as the mechanism to support the adoption of data and cyber security standards across the sector. In doing so the Government response indicated that they would work with councils to support inclusion of this requirement within contracts, work with the CQC to ensure it is part of inspection evidence for social care providers and ensure it is proportionate and appropriately designed for the sector.

   This report has highlighted that further improvements are needed to the toolkit but Government should ensure that the toolkit is seen as the single mechanism for use by adult social care providers. Where providers voluntarily choose to complete Cyber Essentials or other frameworks then there should be continued efforts to reduce duplication of completing the DSPT for those providers (e.g. evidence from Cyber Essentials should pre-populate the DSPT). We recommend that one consistent approach is reinforced and formally recognised by national bodies and commissioners and that the links between the DSPT and other guidance or support materials are made clear (e.g. e-Learning for Healthcare training and National Cyber Security Centre guidance).

Lead organisation(s)	NHSX and NHS Digital

2. **a) Review the content and improve the usability of the Data Security and Protection Toolkit with respect to social care provider completion, and; (b) 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.**

   Context: The toolkit is not designed for small social care organisations. The registration process is complicated and the reduced Entry Level requirements for social care providers are neither clear nor effective. We advise that a review of the content of the toolkit is undertaken to provide assurance that the toolkit is fit for purpose as the single mechanism for providers to self-assess their data and cyber security. We further advise that additional usability testing is undertaken, that signposting (from the toolkit itself) to guidance on completion by social care organisations is put in place, that the Entry level requirements are revised, and that a revised version is available for small organisations. Usability testing should be undertaken with the sector with input from councils and care providers. We recommend that toolkit completion is not made mandatory for social care organisations until these changes are made.

Lead organisation(s)	(a)NHS Digital (b)NHSX

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.**

   Context: Currently, data and cyber security self-assessment - be that the DSPT or information required for tendering/procurement practice - is only a requirement for service providers that contract with the NHS or councils. There is not a mechanism for self-assessment for providers that service the self-funder market. We therefore recommend that completing a revised Entry Level DSP toolkit (subject to recommendation 2) should form part of the evidence inspectors use whilst assessing key lines of enquiry.

Lead organisation(s)	Care Quality Commission

4. **a) Review the existing National Cyber Security Centre guidance on IT security, mobile working and passwords, and b) these should then be promoted by relevant sector bodies to support adult social care providers**.

   Context: There is a wealth of guidance from the National Cyber Security Centre, including the Cyber Security: Small Business Guide, which has a useful infographic that gives a summary of low cost, simple techniques that can improve cyber security within all organisations, and 10 Steps to Cyber Security which would be useful for larger organisations, as well as guidance on Password Security and Home and Mobile Working. There is also guidance available through Digital Social Care's Introduction to Cyber Security. We recommend that national bodies (such as the Care Provider Alliance and LGA) promote this guidance on IT security, mobile working and passwords to raise awareness with the sector.

Lead organisation(s)	(a) National Cyber Security Centre (b) Sector bodies including Care Provider Alliance, LGA

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.**

   Context: Inconsistency of practice between individual CQC inspectors was a key concern for many provider services. The Care Quality Commission should make it clear – on their website or in other publicly available guidance - that they do not require paper records to be kept to aid their inspections, as long as digital records have been implemented in a way that supports the delivery of high quality care. In addition, we recommend that CQC ensures its inspection teams are aware and trained that paper records are not required.

Lead organisation(s)	Care Quality Commission

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.**

   Context: There is widespread uncertainty about data disposal and record retention and a variety of guidance exists. Some providers that are aware of the Records Management Code of Practice for Health and Social Care 2016 and the Retention Schedules question whether these timeframes are appropriate for their data, but are not sure if they are obliged to follow them. For many providers their digital systems and storage arrangements are relatively new, and they have not yet had to think about archiving electronic files. We recommend that one clear and specific adult social care guidance is developed (or endorsed) to help the sector to decide on appropriate retention timescales, and to understand good practice in archiving and permanently deleting electronic records and shredding hard copy ones.

Accountable organisation	NHS Digital in collaboration with ADASS, LGA, Digital Social Care

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.**

   Context: Many providers use specialist proprietary software for care systems and access these systems on-line, hosted in the cloud by the software company. Some of these providers struggle to check their IT supply chain and may not have the clout to enforce changes to the standard terms and conditions offered to them. There is an opportunity to work with providers in proposing a practical approach to support organisations in this area. This may include asking suppliers to complete relevant sections of the Data Security and Protection Toolkit although we understand that other tools may already exist cross-government. (See recommendation 17 for recommendation for care providers in this area).

Accountable organisation	NHS Digital (in collaboration with Digital Social Care)

8. **a) Agree the position across the health and social care system on what constitutes valid evidence of consent in a digital age. (b) Once this position has been agreed, for national partners to promote and advise of this position to respective health and social care organisations.**

   Context: No participating services were entirely paperless, and many highly digital services still printed care or support plans for clients to sign, which were then scanned and the hard copy shredded: rather than capturing electronic signatures (or other forms of consent) directly into digital systems. We are not sure if this is because of technological or cost issues, cultural practice or regulatory requirement, and recommend that this issue is explored further and the benefits of electronic consent made clear. National bodies should advise the sector of this position when it is agreed through a clear, consistent and user friendly approach.

Accountable organisation	NHSX and NHS Digital – with support from sector bodies including CQC, NCSC.

5.2 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.**

Context: Information flow from the NHS to provider services is a key risk for the sector. Not being able to access their clients' relevant NHS records or data and not being able to email NHS organisations was frequently identified as an issue by services, and one that has been previously highlighted by the CQC. Our understanding is that this is a cultural issue, i.e. due to the policy or attitude of the establishments concerned, as much as a technological one. To enable sharing of health records and support integrated working, we recommend that the NHS promotes adult social care provider access to relevant electronic health records, e.g. access to relevant GP information for the people that they are caring for.

Lead organisation(s)	NHS England

10. **Support NHS organisations currently relying on fax for interaction with adult social care providers to use alternative digital channels such as secure email.**

Context: We recommend that the NHS, for example pharmacies, GP practices and continuing healthcare teams, should be supported to phase out the use of faxes and communicate with adult social care services by alternative digital channels such as secure email. This should include supporting provider services to demonstrate that they have a secure email system (see recommendation 18 below).

Lead organisation(s)	NHS England

5.3 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.**

Context: We recommend that councils consider providing, or organising in conjunction with local care associations, specialist data and cyber security advice and services for adult social care services. This could include, for instance, shared access to a Data Protection Officer (DPO), cyber security advice surgeries, support to meet the secure email standard etc. This might be presented as a 'menu' of support available to services, possibly on a charged for basis. As part of this we would encourage councils to accredit local IT support companies and/or to provide outsourced IT support for small local care provider services. For small or new local services councils could provide cyber security training and signposting 'packs' (e.g. Cyber Security: Small Business Guide) or Digital Social Care's Introduction to Cyber Security).

Accountable organisation	Councils (supported by the LGA and ADASS)

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.**

Context: We understand that councils undertake on site checks or audits of services' record keeping and data compliance. These could be extended to encompass a review of services' data and cyber security, based on the questions developed by IPC for the initial 'discovery' visits of this research programme (a summary of the questions used by IPC are shown in the appendix). Crucially, these should not be audits of practice but support by a critical friend to help services reflect on their data and cyber security (and GDPR compliance) and undertake self-assessment.

Accountable organisation	Councils (supported by the LGA and ADASS)

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.**

Context: We recommend that councils check the data and cyber security contractual or tendering requirements (that they ask of service providers) for consistency with other parts of the council (e.g. children's services) and neighbouring/regional councils. In addition, we recommend that the Association of Directors of Adult Social Services (ADASS) and LGA develop guidance for councils so that there is greater consistency of practice based on one agreed national approach (see recommendation 1 above).

Accountable organisation	Councils (supported by the LGA and ADASS) CCGs (supported by NHSE).

5.4 Recommendations for Service Providers

14. **a) 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.**

b) In the meantime, care providers should check their organisation's IT security against the National Cyber Security Centre's guidance.

Context: Completing the toolkit demonstrates compliance with GDPR and the data security standards for health and social care. To complete the toolkit, and to be GDPR compliant, ensure that you have: policies for data protection, quality and security; a privacy notice (for clients, staff and volunteers or visitors if relevant); an information asset register; and a process for dealing with data breaches. Templates and guidance are available from Digital Social Care (www.digitalsocialcare.co.uk/).

Service providers should check their organisation's IT security against the National Cyber Security Centre's Cyber Security: Small Business Guide infographic that gives a summary of low cost, simple techniques that can improve cyber security within all organisations. And if you are a larger business then the 10 Steps to Cyber Security can further help your approach to cyber security. All services should check their cyber security against the key controls in the Cyber Essentials scheme. In particular, ensure that operating system(s) are up to date, and if relevant, upgrade Windows 7 before January 2020.

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).**

Context: We recommend that services review their password security against the National Cyber Security Centre's Password Guidance. If staff or volunteers use smartphones for work, organisations should either develop and implement a BYOD policy and/or 'lock down' organisation provided phones. More information is given in National Cyber Security Centre's BYOD guidance and the NHS Digital Guidance.

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.**

Context: We recommend that all staff and volunteers are supported to maintain awareness of data and cyber security risks and good practice, including training on induction and annual training or awareness raising. This should be in addition to or an extension of mandatory GDPR training for staff. In particular, anyone who works away from the office or home is given the training and the equipment they need to undertake safe mobile working. The Home and Mobile Working guidance that is part of the 10 Steps to Cyber Security as well as Digital Social Care's Introduction to Cyber Security) gives more information.

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).**

Context: Just over half (57%) of participating services used an external person or organisation to provide IT services or support. Usually, IT support companies have administrator access to all records. Internal staff in similar positions are likely to be required to have a satisfactory background check from the Disclosure and Barring Service (DBS). If relevant, we recommend that services undertake due diligence to assure themselves of the suitability of outsourced IT support company personnel. In addition, if relevant, undertake third party GDPR due diligence for all cloud suppliers that provide storage containing personal confidential data and consider asking for evidence that they have Cyber Essential Plus or ISO 2700. Due diligence advice is available from Digital Social Care Guidance on 3rd Party Contracts and Microsoft's Due Diligence Checklist.

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.**

Context: Information flow from the NHS to provider services is a key risk for the sector. Having access to health data and phasing out the use of faxes would both be helped if provider services could demonstrate that they have a secure email system or other secure electronic data transfer method. We recommend that services register the organisation (or individual users) for an NHSmail account through the DSPT (https://digital.nhs.uk/services/nhsmail) or demonstrate that their own email service is compliant with the secure email standard (DCB1596) and register your service with the NHS Digital secure email accreditation process or use a proprietary secure data transfer service. Advice about sharing care records via email is available from Digital Social Care.

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**.

More information is available from Digital Social Care's Business Continuity Plan – Data Security.

6 Appendix: Risk Categorisation Results

Risk categorisation	**Persona type**			**All services**
	One	**Two**	**Three**	
IT security	Green 74% Amber 13% Red 13%	Green 92% Amber 8% Red -	Green 85% Amber 10% Red 5%	Green 84% Amber 10% Red 6%
Physical security	Green 61% Amber 30% Red 9%	Green 86% Amber 14% Red -	Green 81% Amber 19% Red -	Green 76% Amber 21% Red 3%
Mobile device security	Green 22% Amber 30% Red 13% 35%	Green 67% Amber 29% Red - N/A 4%	Green 64% Amber 18% Red 5% N/A 14%	Green 51% Amber 26% Red 6% N/A 17%
Smartphone security	Green 14% Amber 23% Red 18% 45%	Green 61% Amber 22% Red 13% N/A 4%	Green 41% Amber 9% Red 23% N/A 27%	Green 39% Amber 18% Red 18% N/A 25%
Backups	Green 43% Amber 22% Red 35%	Green 83% Amber 17% Red -	Green 95% Amber Red 5%	Green 74% Amber 13% Red 13%
Logins and passwords	Green 24% Amber 38% Red 38%	Green 25% Amber 75% Red -	Green 38% Amber 48% Red 14%	Green 30% Amber 55% Red 15%
Policies	Green 30% Amber 55% Red 15%	Green 42% Amber 54% Red 4%	Green 64% Amber 36% Red -	Green 45% Amber 48% Red 7%
Education and awareness	Green 35% Amber 48% Red 17%	Green 71% Amber 25% Red 4%	Green 71% Amber 19% Red 10%	Green 59% Amber 31% Red 10%
Business continuity	Green 88% Amber 12% Red -	Green 88% Amber 12% Red -	Green 73% Amber 27% Red -	Green 78% Amber 22% Red -
Overall risk	**Green 43% Amber 43% Red 14%**	**Green 83% Amber 17% Red -**	**Green 71% Amber 19% Red 10%**	**Green 66% Amber 27% Red 7%**

Appendix: Data and Cyber Security Programme Discovery Questions

Personal and sensitive information

1. What personal or sensitive data do you collect about the people who use your services? How and where is that data collected and stored?

2. What personal or sensitive data do you collect about your staff? How and where is that data collected and stored?

3. How does the organisation know about and control this data? For example, is there an Information Asset Register or Register of Data Processing Activities? If so, what are the arrangements for updating these registers?

4. How is 'old' information disposed of?

5. How do you inform the people you support, their families and your staff about their information rights and what data of theirs you process? For example, do you have a transparency notice for the people who use your service, staff and/or visitors?

6. Do you have policies for data security, data protection and data quality? If so, are these policies reviewed at regular intervals?

7. How widely are these policies understood and followed?

Data security

8. What information systems do you use?

9. Do you have any plans to change these systems e.g. from paper to electronic, or from one system to another?

10. Which systems (paper or non-paper based) are you most dependent on?

11. What would you do if any of these critical systems went down and you couldn't use them?

12. What things do you do to mitigate your key data security risks?

13. Do you record any of these risks and mitigations? Is this in a contingency plan?

14. Do you have any outsourced IT function in respect of personal and sensitive data e.g. external IT support company or cloud hosted specialist proprietary software system?

15. If so, what do you do to check your IT supply chain to ensure due diligence checks of outsourced IT functions?

Data breaches

16. Would you know what to do if a data breach occurred?

17. Do you have a ‘breach response plan’ or policy?

18. Do you provide guidance to staff on what data ‘breaches’ are and what to do if they suspect one?

19. Have you ever experienced a data breach or been impacted by either a data breach or data related incident in other organisations? If so, what was your learning from the incident(s)?

Keeping your electronic data safe

20. What sorts of IT devices are used by staff in the course of their work? For example, server, desktop computers, laptops, tablets, smart phones, or other devices.

    a) Are these devices supplied by the organisation?
    b) If not, do you have a ‘bring your own device’ policy?
    c) What operating systems are installed on these devices?

21. Which anti-virus software is installed on which devices? Who is responsible for installing it on devices?

22. Does the antivirus software run scheduled scans to check for viruses? Please give details.

23. Are operating system updates (including security patches) applied to devices automatically or manually? What are the arrangements?

24. Is there a network firewall in place?

25. How are laptops and tablets protected to keep data safe when they are used out of the office? For example:
    - Encryption e.g. password protection before the operating system
    - Operating system password
    - Configured to be remotely tracked and/or wiped if lost or stolen
    - Set to automatically update installed (non operating system) software / programmes

26. How are smartphones protected to keep data safe when they are used out of the office? For example:
    - PIN/Password protection/fingerprint recognition
    - Configured to be remotely tracked and/or wiped if lost or stolen e.g. using an app such as Where’s my droid/iphone?
    - Set to automatically update installed (non operating system) Apps

27. Do staff use portable devices e.g. memory sticks, CDs or other removable storage? If yes, how do you ensure those devices are safe to use?

28. Is your data backed up? If yes, what data and how is it backed up and how often?

29. Are the backups tested to see if the information can be restored i.e. disaster recovery testing? Please give details.

30. What email system is used by the organisation? If not NHS mail, is it a secure system? If so, has the system been registered with NHS digital?

Logins and passwords

31. Who adds new users to your electronic systems?

32. When staff login to computers or to systems holding personal or sensitive data, are there any logins which are shared between staff? i.e. one shared login for several staff as opposed to a separate login per person.

33. What are the arrangements for staff changing login passwords? Does the system enforce password changes at regular intervals for example?

34. Do you (or 3rd party applications) impose password policies i.e. how ‘strong’ are your passwords? For example, do you require a mixture of text and numbers?

35. Is two factor authentication used (e.g. tokens, text, App)? Please give details.

36. How many passwords will staff be likely have in total?

37. Is there somewhere safe that staff can keep passwords (e.g. a safe or password manager software such as LastPass, 1Password or a browser password manager)?

38. What happens to staff’s accounts on the system(s), their email address and files when someone leaves or changes role?

Staff and training

39. What training do staff have in: data protection; data quality; data security; and safe use of IT systems?

40. How do you ensure ongoing awareness raising of these issues amongst staff?

41. How confident do you think staff are in:

a) Handling client records and information?
b) Sharing information with external organisations?
c) Using IT systems within the organisation?
d) Using It devices away from the office (e.g. never connect to public Wi-Fi hotspots)?

42. What would increase staff confidence?