Local Authority Adult Social Care Market Cyber Security Survey 2024

March 2025

Introduction

Digital Care Hub launched this survey during Cyber Security Awareness Month – October 2024 - with the aim of asking local authorities in England how they enable contracted adult social care services to follow good data and cyber security practices.

The survey – conducted by the Association for Directors of Adult Social Services (ADASS) regional teams and Digital Care Hub's *Better Security, Better Care* programme – explores what data protection requirements are included in local authority contracts, how aware local authorities are of any requirements, how they monitor compliance and what sorts of additional support would be helpful. The survey is a response to the increased cyber security risks faced by the public sector and the adult social care services they commission. ADASS regional teams have supported Digital Care Hub in designing and promoting this survey amongst local authorities in England.

Our goal is to understand what mechanisms are used to ensure that care providers are equipped to handle potential data breaches or cyber-attacks, as well as explore what else might help councils to work with care providers securely in the future. The findings will be used to identify what resources and support could be made accessible to local authorities to help them strengthen data and cyber security measures throughout commissioned care services.

"Data and cyber security are critical components of a robust social care system. As we increasingly rely on digital solutions, it's imperative that all partners in the social care ecosystem work together to strengthen our defences against potential threats. This project marks an important step in understanding and improving the measures currently in place," said Michelle Corrigan, Programme Director of Better Security, Better Care.

"Our collaboration with ADASS regions will help ensure that the sector is resilient and prepared to protect sensitive information effectively. We are pleased to be leading on this important piece of work," said Mark de Bernhardt-Lane of South West ADASS.

Mark also added, "We know that cyber attacks are becoming more common and that those attacks are likely to increase. We can all play our part in improving cyber security and reducing the risk and impact of attacks. This partnership with Better Security, Better Care will help councils identify good practice and what else can help when working with care providers to strengthen data protection arrangements."

Executive Summary

This survey, conducted by ADASS regional teams in collaboration with Digital Care Hub's *Better Security, Better Care* programme, aimed to explore how local authorities in England enable contracted adult social care providers to follow good data and cyber security practices. With growing cyber security risks across the public sector, the survey sought to understand the mechanisms used by councils to safeguard sensitive data, ensure compliance, and identify areas where additional support might be needed. By identifying gaps and opportunities, the findings will inform strategies to strengthen data protection and cyber resilience in adult social care services.

The survey investigated what data and cyber security requirements are included in local authority contracts with care providers and how compliance is monitored. It also examined awareness and usage of existing free resources provided by the *Better Security, Better Care* programme. The ultimate aim is to ensure care providers are better prepared to handle potential data breaches or cyber attacks, while helping councils develop stronger working relationships with providers. The findings will guide the creation of tailored resources and support to enhance data and cyber security measures across commissioned care services.

Key findings

While the survey uncovered many important insights, the summary focuses on a few key findings:

- **Participation and roles**: The survey received 55 responses from a broad cross-section of local authorities, representing 36% of eligible councils. Most respondents were commissioners (60%), with the remainder including roles in procurement, quality assurance, and digital leadership.
- **Awareness of resources**: While many respondents were aware of *Better Security, Better Care*'s free resources, nearly half were unaware of specific tools available to them, highlighting the need for greater awareness.
- **Cyber security gaps**: 16% of local authorities reported having no formal cyber security or data protection requirements in contracts, and 22% were unsure of their arrangements. Cyber security emerged as the weakest area of confidence compared to data management.
- **Support needs**: 60% of respondents expressed a desire for additional free support from *Better Security, Better Care* Local Support Organisations to monitor compliance and improve quality. However, 27% were unsure, and 13% did not see the need for further assistance.
- **Collaboration challenges**: Only 44% of respondents reported regular communication with their Integrated Care Boards (ICBs), a key factor in improving data security practices.

Recommendations and conclusion

To address the identified gaps and improve data security practices, several actions are recommended.

- Regular engagement between ADASS regional leads, the Digital Care Hub team, and local authorities should be established to provide continuous updates on available resources and address challenges like staff turnover.
- The pilot of ADASS Regional Digital and Cyber Leads should be expanded to all regions.
- Promoting the *Better Security, Better Care* resources more widely through newsletters, webinars, and tailored communications will help ensure that all councils are aware of the tools at their disposal.
- Strengthening collaboration between Integrated Care Boards (ICBs) and local authorities is also essential, as areas with stronger ICB-local authority

relationships have shown higher compliance and greater awareness with implementing robust cyber security measures.

- Local authorities requesting further assistance from Better Security, Better Care should be contacted directly to provide bespoke guidance and training.
- Developing training initiatives such as webinars on cyber security drills, recovery planning, and practical steps to respond to cyber attacks will help build the necessary capacity and resilience to address evolving threats.

This work is critical to addressing the increasing risks posed by cyber attacks in the adult social care sector. By implementing these recommendations, local authorities can enhance their resilience, protect sensitive data, and support care providers in meeting modern data security challenges. Strengthened collaboration and access to tailored resources will create a more robust framework for safeguarding vulnerable populations and ensuring continuity of care in the event of cyber incidents.

Acknowledgements

We extend our sincere thanks to the ADASS regional leads for their invaluable support in promoting and sharing this survey. Their contributions have been instrumental in gathering the insights needed to drive meaningful improvements in data and cyber security practices across adult social care services. We also extend our thanks to the local authorities who gave their views and helped to form the bulk of this report.

Feedback

We welcomed feedback on this report from Connor James, advisor in Digital Transformation for the Local Government Association (LGA) and Partners in Care and Health (PCH).

"As Partners in Care and Health, alongside ADASS regions, the Local Government Association welcomes and supports this report, that provides a valuable understanding into the current data and cyber security measures our local authorities have in place.

"As digital transformation accelerates across the sector, and the risk of cyber security incidents increase, our collaboration with Digital Care Hub and the Better Security, Better Care team is essential in ensuring that our local authorities are equipped with the necessary tools and guidance to safeguard sensitive information.

"By collaborating on these efforts, we are taking significant steps toward strengthening the sector's resilience in data and cyber security."

Methodology

Survey structure and design

The survey was designed to gather insights into how local authorities in England are enabling adult social care providers to follow good data and cyber security practices. It aimed to assess awareness of available resources, the level of confidence in data and cyber security practices among providers, and the extent to which local authorities are incorporating data security requirements into their commissioning processes.

The survey was distributed via Microsoft Forms and was open for responses from 10th October 2024 to 15th November 2024. A total of 55 responses were collected.

The survey was structured to include a combination of multiple-choice, Likert-scale, and open-ended questions. This approach allowed for both quantitative data collection on awareness, confidence, and support needs, as well as qualitative feedback on specific challenges and resource needs. Key themes included knowledge of the *Better Security, Better Care* programme resources, awareness of the Data Security and Protection Toolkit (DSPT), and the extent of collaboration between local authorities and Integrated Care Boards (ICBs).

Survey distribution

To maximise participation, the survey was widely promoted through multiple channels. These included the Fortnightly Digital Care Hub Newsletter and the Weekly Local Support Organisation Email, which reached a broad audience across the adult social care sector. Additionally, an email was sent to all ADASS regional leads across the country, requesting their support in sharing the survey with their networks. Follow-up meetings with the regional leads were held to keep them updated on the survey progress and encourage further engagement from councils who were yet to participate.

The regional leads then distributed the survey within their own networks, whilst the Digital Care Hub team promoted it through the Local Government Association (LGA) Partners in Care and Health leads and local press outlets. This multi-layered approach was designed to ensure the survey reached a diverse group of stakeholders involved in the oversight and commissioning of adult social care services.

Data analysis

Once the survey closed, the responses were analysed to identify key trends, gaps, and areas of concern. Quantitative data from multiple-choice and Likert-scale questions were analysed using descriptive statistics, such as frequency counts and percentages, to identify patterns in responses. This allowed for an understanding of the level of awareness, confidence, and support needs among respondents.

Qualitative data from open-ended questions were analysed thematically. Responses were reviewed to identify recurring themes and key insights, particularly around challenges faced by local authorities and the types of resources they found most useful. This qualitative analysis provided a deeper understanding of the context behind the quantitative findings and helped to identify specific areas where further support may be required.

Analysis

It is encouraging to note that 55 local authority areas filled out the survey, representing a broad geographical spread across the country. This is out of a possible 151 Local Authority areas with CQC registered Adult Social Care services, resulting in a strong sample size of 36% of eligible Local Authorities.

See Appendix 1 for a list of questions, and Appendix 2 for responses.

Accessing Better Security, Better Care support

Of the respondents, 60% of those that answered held a commissioner role, while 9% worked in contracts and procurement, 7% in quality assurance and the remainder spread evenly between digital lead, director and quality assurance roles within the Local Authority. The majority of those that answered were aware of the free resources offered by the Better Security, Better Care programme and had shared them with their networks. However, a deeper analysis of individual resources revealed that nearly half of respondents were still unaware of some offerings. This highlights areas where further promotion and awareness raising may be needed. See below for a more detailed breakdown:

Table 1

Resource	Aware	Aware and Shared	Not Aware
Better Security, Better Care **Local support Organisation**	41.8%	29.1%	29.1%
Free Webinars	34.5%	40%	25.5%
Free online guides to complete DSPT	32.7%	36.4%	30.9%
Free national helpline	23.6%	47.3%	29.1%
Template policies and procedures	32.7%	21.8%	45.5%
Free elearning	34.5%	27.3%	38.2%
Template wording for contracts with ref to DSPT	30.9%	16.4%	52.7%

Single Assessment Framework

When asked about the Single Assessment Framework, it was reassuring to note that 67% of respondents were aware that the Care Quality Commission (CQC) have included the DSPT as a requirement in the Single Assessment Framework. However, it is notable that a third of respondents were not aware of this development. A similar trend was observed regarding the What Good Looks like framework, which recommends the DSPT as a contractual and commercial requirement when commissioning adult social care. While 69% of respondents were familiar with this recommendation, 31% remained unaware.

Confidence in care providers

Additionally, it was encouraging to see that local authorities generally expressed confidence in the ability of care providers in their area to manage data effectively. However, it is concerning that the management of cyber security emerged as the weakest area in terms of confidence, as shown from the further breakdown in Table 2.

This may be due to the evolving nature of cyber threats, which often outpace the ability of care providers to implement comprehensive and up-to-date security measures. Many providers may also lack the technical expertise or resources to address increasingly sophisticated cyber risks, which can result in gaps in their security practices. This highlights a potential area of vulnerability, particularly as the digital landscape continues to expand and cyber attacks become more prevalent.

In addition, it is concerning that only 29% of respondents felt confident that care providers in their area had a robust data and cyber business continuity plan in place. This low level of confidence could be attributed to two possible factors. On the one hand, local authorities may not have asked care providers about the cyber aspect of a provider's continuity plan, which means they may not be fully aware of whether providers have comprehensive plans in place to safeguard against cyber threats. On the other hand, the providers may lack the necessary plans to address cyber risks adequately, which suggests a potential gap in preparedness. In either case, the lack of confidence highlights an area of concern, as the absence of strong continuity planning could leave care providers vulnerable to cyber incidents, ultimately affecting both data security and service continuity.

Table 2.

Resource	Not Confident	Not so confident	Somehwhat confident	Confident	Very confident
Manage confidential data	7.3%	0%	54.5%	34.5%	3.6%
Use secure email systems	3.6%	7.3%	50.9%	34.5%	3.6%
Manage cyber security	1.8%	21.8%	58.2%	18.2%	0%
Robust business continuity plan in place	1.8%	14.5%	45.5%	29.1%	9.1%

Contracting requirements

When asked if they had cyber security and data protection requirements within their adult social care commissioning contracts or quality monitoring (table 3), it is alarming to see 16% had neither DSPT or Cyber Essentials as part of this process and 22% did not know. The absence of these frameworks in commissioning contracts suggests a significant vulnerability in the safeguarding of sensitive information, not only for care providers but also for the local authorities that share data with them.

Furthermore, the fact that 22% of respondents were unaware of whether these requirements were in place points to a potential gap in oversight and accountability. Local authority staff play a critical role in regulating and supporting care services, and their knowledge of contractual requirements is fundamental to ensuring the resilience of the sector against cyber attacks.

Table 3.

Resource	Not Confident

I do not know if we have DSPT or Cyber Essentials (or equivalent) in our contracts with commissioned Adult Social Care providers	22%
We have neither DSPT or Cyber Essentials (or equivalent) in our contracts with commissioned Adult Social Care providers	16%
Yes, we have both DSPT and Cyber Essentials (or equivalent) in our contracts with commissioned Adult Social Care providers	22%
Yes, we have Cyber Essentials (or equivalent) but NOT DSPT in our contracts with commissioned Adult Social Care providers	11%
Yes, we have DSPT but NOT Cyber Essentials in our contracts with commissioned Adult Social Care	29%

Future support from Better Security, Better Care

When asked how the programme could support local authorities, 60% of respondents answered that they would welcome free support from the *Better Security, Better Care* Local Support Organisations in monitoring DSPT compliance and quality in their area. 13% would not, and 27% were unsure.

This indicates a strong demand for assistance, reflecting a recognition of the challenges that local authorities face in ensuring care providers meet robust data security standards.

However, it is notable that 27% of respondents were unsure whether they would benefit from such support. This uncertainty may stem from a lack of clarity about the scope and value of the assistance offered by the *Better Security, Better Care* Local Support Organisations, or from a limited understanding of their role in monitoring compliance and quality. Bridging this knowledge gap through targeted communication and case studies could help demonstrate the tangible benefits of utilising *Better Security, Better Care* support.

The word cloud below shows what additional support ideas specifically aimed at councils respondents felt would be useful:

Integrated Care Boards (ICBs)

When asked about their communication with Integrated Care Boards (ICBs), only 44% of local authorities reported having regular communication, while the majority, 56%, did not. This lack of regular interaction is concerning, given the role ICBs play in supporting social care as part of their remit within the NHS. The absence of consistent dialogue suggests missed opportunities to strengthen these partnerships, which could leave gaps in understanding and undermine efforts to create a cohesive system of care.

Areas with strong ICB-local authority relationships often see better coordination, which can lead to improved compliance with frameworks like the DSPT. Strengthening these links could help local authorities and ICBs to link in better with Digital Care Hub and the resources on offer.

Conclusion and Recommendations

The survey responses highlight a strong demand for continued support in data and cyber security within adult social care, particularly with regard to the DSPT. This reinforces the need for tailored resources and guidance to support local authority teams to work effectively with care providers, in efforts to ensure that sensitive data remains secure and services remain resilient against cyber threats.

The following recommendations outline actionable steps to address the key findings and improve support for local authorities:

1. Regular engagement with local authorities

Establish regular meetings between ADASS regional leads, Digital Care Hub (DCH), and local authorities to provide updates on available resources, ensuring that all staff, including new recruits, are kept informed. Explore opportunities to integrate Digital Care Hub support into regional commissioner meetings to enhance collaboration. Recently in 2024, the Engagement Team at DCH have been meeting on an individual basis with different local authority areas which has seen huge improvements of engagement with the DSPT. These meetings are a result of the wider commissioner network groups.

Digital Care Hub are currently piloting "Data and Cyber Security Health Checks" in the Southwest with promising early results. The pilot will conclude in March 2025 and should be rolled out as a service Local Support Organisations can offer from mid-2025 onwards to help adult social care providers externally assure themselves. Digital Care Hub should reach out to Local Authorities who were interested in this activity being rolled out in their area and prioritise these areas as they are the most likely to participate.

2. Increase awareness of frameworks and standards

Continue to increase awareness of CQC's Single Assessment Framework and the What Good Looks Like framework, particularly their connections to the DSPT.

3. Clarify DSPT and Cyber Essentials

Continue to educate local authorities on the distinct benefits of DSPT and how it differentiates from Cyber Essentials whilst still emphasising the importance of both. Continue signposting to Digital Care Hub online resource in efforts to encourage local authorities to consider their commissioning contracts to enhance cyber security and data management.

4. Resource Promotion and Accessibility

Actively promote new and existing resources from the Digital Care Hub through newsletters, case studies, and targeted campaigns. Ensure materials are tailored and easily accessible to local authority staff. For example, taking some key stats from this survey and developing materials to share with councils.

5. Strengthen collaboration between ICBs and local authorities

DSPT compliance is typically higher in areas where strong relationships already exist. Encouraging ICBs to establish stronger working relationships with local authorities will help the sector to improve their cyber resilience. Highlighting successful case studies where collaboration has led to higher DSPT publication rates and greater resilience against cyber attacks is one example of how Digital Care Hub could help steer some of this.

6. Business Continuity Plan campaign

Advocate for local authorities to require robust cyber and data business continuity plans as part of care provider contracts. Given that only 29% of local authorities expressed confidence in the existence of plans amongst commissioned services, working with them to understand how the DSPT can make them a contractual obligation will ensure better preparedness and accountability.

7. Targeted outreach to "unsure" respondents through ADASS regions

Focus outreach and support efforts on the 27% of respondents who were unsure whether they needed additional support from *Better Security, Better Care* LSO's. Tailored engagement could clarify their specific needs and barriers, potentially opening some new avenues for our engagement. This can be curated by Digital Care Hub and disseminated through the ADASS regions with a high proportion of 'unsure' respondents.

8. Collaboration with Local Government Association (LGA)

Partnering with the LGA to co-develop strategies and resources could amplify the importance to local authority colleagues. In the Southwest and West Midlands there have been successful pilots of Digital ADASS Leads who encompass cyber, tech and digital into one role. Expanding this pilot to other ADASS regions would increase capacity within the existing infrastructure to greatly increase the awareness of cyber security issues within local authorities and allow them the space to collaborate with each other and the broader digital ecosystem. Individually contact those who wanted more free support tailored to their Local Authority. Create, develop and promote easy to understand webinars for Local Authorities specifically on data and cyber security, in partnership with the Local Government Association and ADASS regional leads.

9. Secure email adoption

Local authorities showed awareness and confidence that care providers have access to secure email systems. This is contrary to research commissioned by Digital Care Hub which found that around half of providers had access to NHSmail and most would only use it in a limited capacity to communicate with partners in the NHS. More support is needed to care providers and local authorities to increase the adoption of secure email systems such as NHSmail and clarify use cases for providers and commissioners in local authorities.

Progress to date

Over the past three years, Digital Care Hub has worked in close collaboration with ADASS regions and local authorities to improve data and cyber security practices across the adult social care sector. This partnership has grown significantly, with focused support now provided to commissioner groups within the regions.

These efforts have demonstrated the value and importance of regular meetings and ongoing collaboration, as highlighted in the recommendations of this report. The commitment to continuing this work remains a priority, ensuring that new staff members and evolving teams are kept informed of available resources and initiatives.

As part of Better Security, Better Care, the North West ADASS region developed a document to support adult social care commissioners with contracting adult social care services. This resource includes example contract wording that incorporates DSPT requirements and guidance on monitoring provider compliance. This practical tool has been helpful in encouraging the inclusion of DSPT requirements in adult social care contracts.

A range of additional resources and tools are already available to support local authorities in supporting care providers to strengthen their data and cyber security practices. These include:

- **Case Studies**: Access to a collection of case studies showcasing best practices and innovative approaches taken by other councils, available on the Digital Care Hub website.
- **Local Support Organisations:** LSOs can provide monthly reports detailing provider compliance levels within each local area, enabling councils to monitor progress effectively.
- **Tailored DSPT resources developed by councils:** Guidance on auditing Business Continuity Plans to support councils with monitoring data and cyber security processes of commissioned providers.
- **LGA Data Protection and Cyber Security Guidance for Commissioners:** Guidance includes how to support care providers to complete the Data Security and Protection Toolkit.
- **E-Learning for frontline staff:** Free, accessible data and cyber security e-learning modules designed specifically for frontline care staff that councils can signpost commissioned care services to.
- **E-Learning for Data Protection Leads:** Free, accessible data and cyber security e-learning modules designed specifically for data security protection leads that councils can signpost commissioned care services to.
- Please sign up for our fortnightly newsletter where you will find funding opportunities, **Newsletter Signup | Digital Care Hub.**

Appendix 1 Questions

Questions from the survey can be found below:

1. Which Local Authority area(s) does your work cover?

2. What role do you have within your Local Authority?

3. Are you aware of the following free support from the official DHSC-funded Better Security, Better Care Programme supporting providers with the Data Security and Protection Toolkit (DSPT)? Have you shared these with care providers?
    a. Better Security, Better Care Local support organisations
    b. Free webinars on the DSPT
    c. Free online guides on completing the DSPT
    d. Free national helpline
    e. Template data protection policies and procedures
    f. Free elearning
    g. Template wording for contracts with care providers, with reference to DSPT

4. Were you aware that CQC have included the Data Security Protection Toolkit (DSPT) as a requirement in their Single Assessment Framework?

5. Are you aware that the What Good Looks Like framework for digital working in adult social care recommends the DSPT as a contract and commercial requirement when commissioning Adult Social Care services?

6. How confident are you that the majority of care providers in your area:

    a. Manage confidential data

    b. Use secure email systems

    c. Manage cyber security

    d. Robust business continuity plan in place

7. Do you have cyber security and data protection requirements within your adult social care commissioning contracts or quality monitoring? E.g. DSPT and/or Cyber Essentials or equivalent?
    a. Yes, we have both DSPT and Cyber Essentials (or equivalent) in our contracts with commissioned Adult Social Care providers

b. Yes, we have DSPT but NOT Cyber Essentials in our contracts with commissioned Adult Social Care providers

c. Yes, we have Cyber Essentials (or equivalent) but NOT DSPT in our contracts with commissioned Adult Social Care provider

d. We have neither DSPT or Cyber Essentials (or equivalent) in our contracts with commissioned Adult Social Care providers

e. I do not know if we have DSPT or Cyber Essentials (or equivalent) in our contracts with commissioned Adult Social Care providers

8. Would you welcome free support from your Better Security, Better Care Local Support Organisations in monitoring DSPT compliance and quality in your area?

9. What additional resources aimed directly at councils (e.g. webinars, case studies, template letters, testimonials) would be helpful to understand and promote good cyber and data security with care providers.

10. Do you or your colleagues have regular communications with your local ICB where digital security/DSPT is assessed?

11. What ICB job role(s) do you or your colleagues communicate with and what subjects do you cover?

12. If you would like to be put in contact with Digital Care Hub to receive free support, help and guidance tailored to councils, please leave your email address for us to be able to contact you.

13. Please enter your email address if you would like to opt-in to our fortnightly Digital Care Hub newsletter.

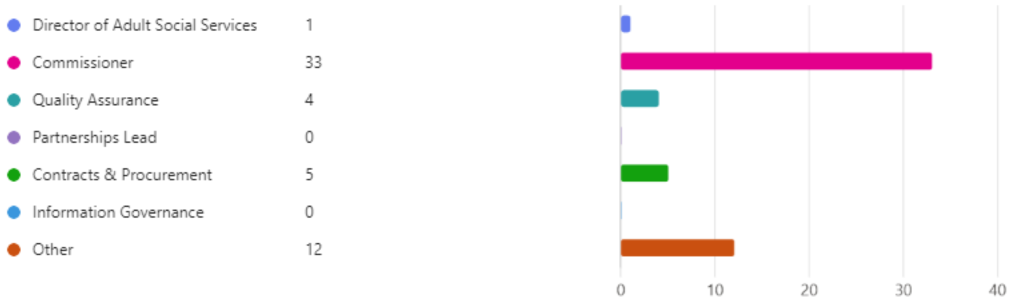
Appendix 2 – Responses

Question one asked what local authorities did the responder come from.

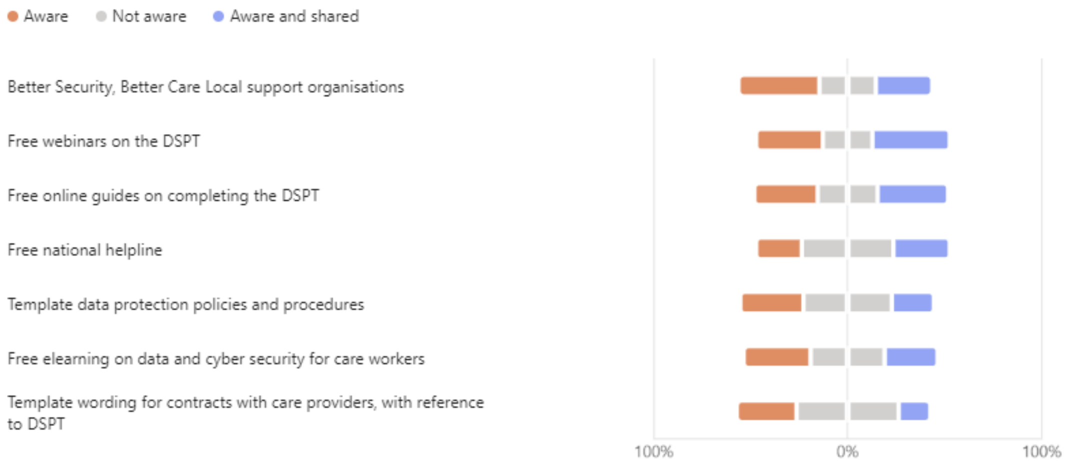
Worcestershire
Wirral Council
Lancashire
Oldham Council
Kirklees
Trafford
Leicester City council
Derbyshire
Adult Social Care- Residential and Nursing care homes
Derbyshire County Council
ASC
Southampton
West Northants Council
Lancashire County Council
Kent County Council
Royal Borough of Windsor and Maidenhead (RBWM)
Isle of Wight Council
Bracknell Forest
Buckinghamshire Council
Tameside MBC
Cambridgeshire County Council
Sandwell
Blackburn with Darwen
Essex County Council
Cambridgeshire
East Sussex
Durham County Council
Barnsley
Dudley
Brighton and Hove City Council
Lambeth
Barnsley Metropolitan Borough Council
Surrey County Council
Wolverhampton
City of Wolverhampton Council
Portsmouth

Telford and Wrekin
North Tyneside Council
Cumberland Council
North Yorkshire Council
Bolton Council
Cheshire West and Chester Council
Gateshead
Coventry
Milton Keynes City Council
Middlesbrough
Suffolk and North East Essex
Leeds
Liverpool
Hampshire County Council
Derby City Council
Wolverhampton
Rotherham Metropolitan Borough Council
Solihull Council
Oxfordshire

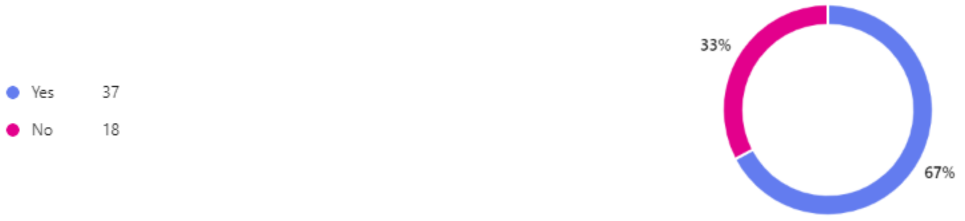
Question two asked what role did they have within their Local Authority?



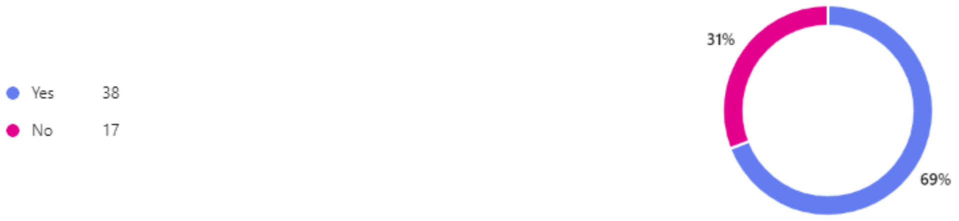
Question three asked if they were aware of the free support available to them through the Better Security, Better Care website which supports providers to complete the Data Security Protection Tool (DSPT), and if they had shared these with care providers.



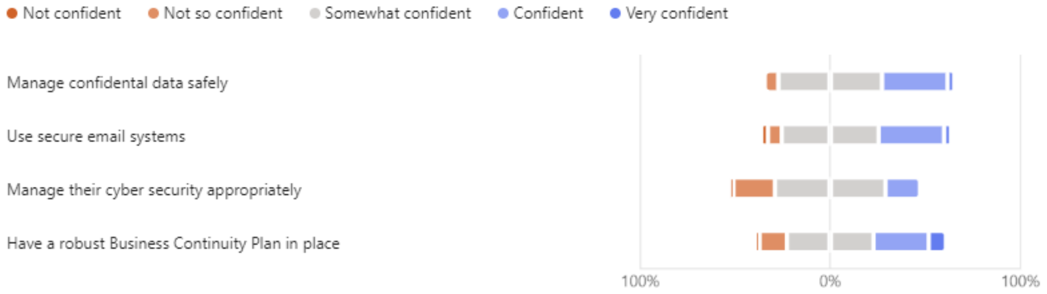
Question four asked if they were aware that CQC had included the DSPT in the Single Assessment Framework.



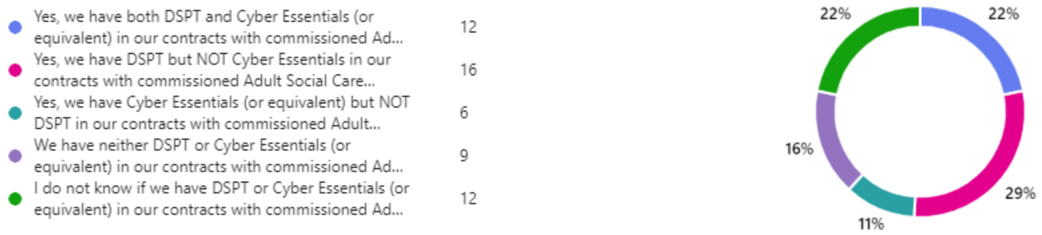
Question five asked if they were aware that the What Good Looks Like Framework recommends the DSPT as a contract and commercial requirement when commissioning Adult Social Care services.



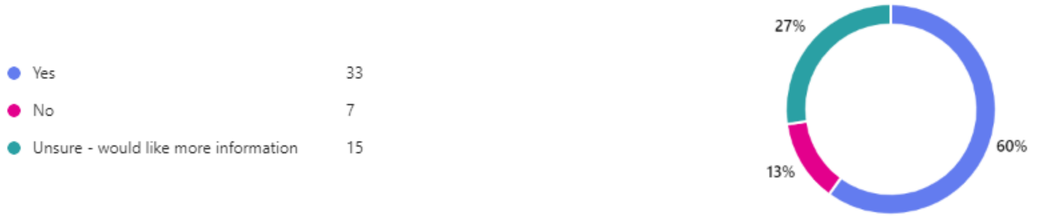
Question six looked at the confidence of care providers in their area on different areas.



Question seven asked if their local authority had cyber security and data protection requirements within their adult social care commissioning contracts or quality monitoring. E.g. DSPT, Cyber Essentials or equivalent.



Question eight asked if they would welcome free support from their Better Security, Better Care Local Support Organisation in monitoring DSPT compliance and quality in their area.



Question nine asked what additional resources aimed directly at councils (e.g. webinars, case studies, template letters, testimonials) would be helpful to understand and promote good cyber and data security with care providers.

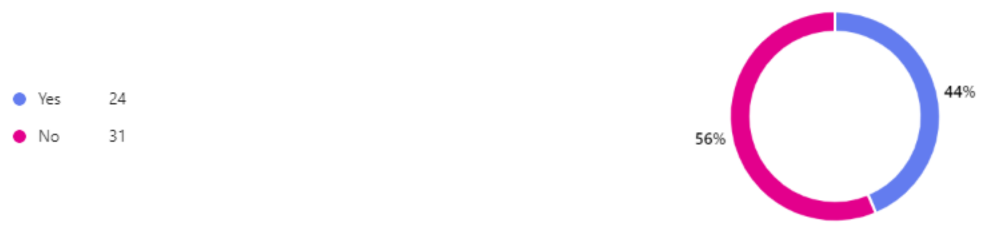
Advice and guidance to support smaller care providers to transition from webmail to NHSmail - in similar way to how the DSPT compliance support has been provided. In Wirral, this would close the cybersecurity loop, ensuring that secure email is used by default. Work will have to be done at a national level with larger providers as they utilise their own email domains and the current NHSmail system for social care providers is restricted to 10 separate addresses - larger providers will need more addresses or a different route to obtain NHSmail accounts.
That all sounds great, thankyou.
Given the stretched capacity in Local Authorities i would welcome 'LSOs' conducting data security checks, their specialisms in this field is valued and would mean that any additional training for LAs to conduct 'in house' could be avoided and their role would be overseeing. Case Studies would also always be welcomed.
Support driven by Care Association into the sector is far stronger and better received than that led by the Council. Care Associations are well placed to respond collectively about issues and share good practice.
unsure
it would be helpful if these were available to providers
Template Letters and Webinar training for Local Authority staff.
a webinar would be helpful
More information around the whole area, it's very vague.
The example of funding to local organisations would be welcomed. We tend to rely on colleagues in the ICB and local care provider organisation to provide support and guidance.
"data security health-checks" and "Business Continuity Plan Drills"
Dedicated, in-person support for our smaller regulated care providers to complete the DSPT. It can be very onerous and too technical for some private care providers.
webinars
Webinars and templates
Any additional would be useful
Data security health checks and Business Continuity Plan templates

We already work very closely with our local support organisation to support good practice around data and cyber security. This has been recognised in a case study published on the Digital Care Hub website: https://www.digitalcarehub.co.uk/success-story/how-social-care-partners-are-working-together-to-improve-data-and-cyber-security-infrastructure/ Some of the answer options in this questionnaire do not allow us to answer accurately, so additional explanation is provided here: - Q7: Historically these requirements have not been in contracts but as we recommission services and contracts are updated, this is something we are adding. Therefore the picture is currently mixed but will continue to improve as we recommission provision. - Q8: We already make good use of this support. We consider this to be a fantastic and valuable offer for providers.
Webinar for commissioners for what to include and check for DSPT and cyber security - in plain English, including any ongoing monitoring
The health checks would be very helpful. Having somebody who can make suggestions on improvements.
Sample contract wording, conducting Data Security Health Checks and Business Continuity Plan drills, template letters to providers with links to guidance and CQC info, webinars
Recommendations on best practice by other councils that supports us to check and align activities in this space. Clarity of what is required of the authority when it comes to engaging with providers. It would good to have this in a template or check list.
all the suggestions sound positive and think would be welcomed, particularly from smaller and VCS organisations that often don't have the resources to produce themselves.
All of the above would be helpful. It is helpful if organisations can access things at a time convenient to them e.g. recordings.
Case studies and template letters
All of the above
The above would be extremely helpful
Recovery planning
I am not involved in business continuity planning
Support around planning and carrying out Cyber Security drills and guidance / best practice on data security health-checks including a focus on fail safe back up arrangements for key client care record systems to enable critical service continuity in the event of a major outage of systems arising from Cyber attacks
As a council we have our own IT department who take cyber security seriously and we have regular training and updates on the matter. In my role I am also working with the West Midlands Care Association and our Commissioners to raise awareness od DSPT.

I think ASC providers are unclear as to the benefits, and perceive threat with change. I think all ASC Provider Directors should have an understanding of Integrated Care Systems and Public Policy related to the Health and Care Act (2022). I think ASC Directors should be actively communicated with by localised NHS Service providers - and ensure they understand why operating with an NHS email account is significant to future Information Sharing needs - and needs related to providing the Health and ASC services to people as they age and die.
Webinars, case studies (however we would still require the funding support providers through the care association)
We currently work with Partners in care to deliver DSPT compliance and training
Data updates on providers that are registered and have met DSPT / Cyber Essential requirements so we can target those that have not, we will also check our contracts on this and include as appropriate, thanks
A webinar series would be useful and possibly examples of good practice which we would be able to share with Providers
Business Continuity Plan Drills would be of benefit to the care market in North Yorkshire
Health checks and some webinars would be a great addition, as a council we have tried to encourage people to sign up to these resources but struggle to reach out. I would suggest something more proactive rather than just giving advice via forums i.e.. the “data security health checks” that they have mentioned would be a great input but any other resource would be a massive help to our providers.
Attendance at Provider Forums and/or specific Provider comms.
Within the council plans are being developed in relation to council led services.
webinar series, case studies, template letters, testimonials data security health-checks and Business Continuity Plan Drills
Not known yet
We receive regular reporting of the DSPT status of the registered providers 'in area'. However it would be useful to receive bespoke reporting for all of the other providers we contract with 'out of area'. It also would be useful for support to be offered to providers who are not registered with CQC - such as the same equivalent support being offered the housing providers, DA, providers. We are entering a digital age for care planning so probably training quick guides that are easy to follow. We still have some people working in the private care sector that cannot use technology very well. The digital maturity of the workforce is quite variable.
Personally, i think there is a wealth of material for care providers and the organisations within our patch are working really hard with care providers to support the DSPT completion and Cyber awareness

Those webinars sound like a very good idea.
I am happy with the support already provided
Webinars and case studies
I think all of the things mentioned would be helpful, but particularly anything that offered providers a way of sense checking their services and systems are up to spec such as the data security health-check or drills.
I believe it would be beneficial to host practical sessions that would scope out legislative requirements for both providers and Councils, to then compare it against new developments in the area (e.g. CQC Single Assessment) and solutions available on the market. This will allow Councils and Providers to compare where they currently are, where they should be and how they can get there.
Case studies
Unsure
Both Health Checks and Business Continuity Drills would be welcome. Formal certification associated with the eLearning - so providers can highlight that they have complied.

Question ten asked how if they had regular communications with the ICB where digital security/DSPT is assessed.



Question 11 asked what role and what subject did they communicate with their ICB on?

Digitisation in regulated care steering group
Associate Director Quality and Safety (Oldham)
Digital Project Manager, Head of Technology - discussing DSPT, partnership working, DSCR projects.
Quality Lead re Clinical Input Referrals
Unsure

ICB Commissioners, Health professionals, Safeguarding and Contract managers.
ICB Commissioners and quality teams
Anyone within ASC or that area.
We work with Hampshire and Isle of Wight ICB, Digital Social Care Team - https://www.hantsiow.icb.nhs.uk/your-health/schemes-and-projects/digitalsocialcare
Digital Lead DSCR update AT pilots
Lancashire and South Cumbria Digitising Social Care Team - DSPT, DSCR, and secure mail.
Digital Transformation Team (they lead on digitizing social care programme)
Health Commissioning - funding is the issue.
Commissioning
Not Sure
Our local support organisation provides the Council's commissioning service with monthly DSPT compliance data. Commissioners use this to support conversations with providers who are not compliant with the DSPT. Compliance, and broader cyber security issues are discussed monthly through the commissioning service Quality Monitoring Group and any key messages and learning is then shared via our monthly system Quality Surveillance Group. This includes partners from across the health and social care system including from the ICB the Quality and Patient Experience Senior Manager; Designated Nurse Safeguarding Adults; Quality Manager Primary Care.
Comms tends to be with operational colleagues rather than corporate
N/A
Better Care Fund Team, Digital Transformation Fund
Equivalent quality lead and clinical lead
IT Leads and Senior Cyber Staff across ICB organisations. We meet regularly and also have informal as and when required.
commissioners - learning disablities, mental health and autism
We are part of an integrated team so we communicate with ICB colleagues regularly across a range of topics. The LA employed staff lead on provider digital work (under Supporting the Provider market team) but our head of service (ICB Director of Delivery) has supported with funding and sign off for our integrated digital initiatives. In terms of digital issues, we work closely with the ICB Digital Lead at place – to discuss NHSmail issues, proxy access issues.
DSPT and NHS email
Health Commissioners - Joint commissioning- safeguarding- quality assurance
Commissioning, Quality and Data Colleagues
ICB Digital and IG leads
I do not communicate with ICB

There is to be an LRF exercise next year based on Cyber which will involve the ICB but at this stage we are not able to provide specific names and roles of individuals working specifically on Cyber Security.
Digital Leads and Digital Director for the ICB
We have a new Head of Adults Commissioning who directly represent NHS Black Country ICB. Her role is towards joint commissioning and Integrated Care Services. Data Security Protection Toolkit registration has not been discussed with our wider team yet, although I have actively shared information with her regarding the need further to a WMCA DSPT webinar explaining the need.
Digital Programme Manager for NHS HIOW
Digital lead and Clinical lead
Commissioners
ICB Director of Delivery - Hospital Discharges and System Integration Group Project Officer and Business Administration - Accident and Emergency Delivery Board (AEDB)
Commissioning and Finance
I don’t have any direct communication with the ICB.
Unsure
ICB Quality and delivery
Digital Data Board, CIO - Digital and system developments across Health and Social Care, ICR, Digital Strategy
The main topic of discussion with the ICB is around finance/payments/recharges. We do however also liaise re: service developments, quality issues - good and bad, void management in supported living, case management queries - particularly those who are joint funded/S117, cross-LA commissioning activity.
Digitising social care records programme and project management, dspt, cyber, digital social care records
Generally, BCF/S75 commissioning and operations, LD/MH Older Adults.
Frailty and programme leads to discuss prevention and TEC
Quality Assurance and Safeguarding Adults Team - regular meetings / joint visits to providers. Information gathering and intelligence sharing.
Mainly health partners or colleagues from key workers to managers, generally covering the subject of individuals care and support needs, budgets and annual uplifts.
Unfortunately, being relatively new to my role at Wolverhampton I am still learning the internal staffing system and how it links with the ICB locally. However, I am aware that my colleagues have regular communications with the ICB and they also discuss digital security.
ICB Commissioners
ICB Director of Digital through the Digitising Social Care Programme, and attend oversight group across health and social care

Jointly commissioned services - performance, personnel and finance
Joint Commissioner Exec board - strategic developments, legislative change, challenges

Question 12 asked who would like to put in contact with Digital Care Hub to receive free support, help and guidance tailored to councils. 35 out of the 55 respondents answered said they would like to be signed up.

Question 13 asked who would like to be signed up to the Digital Care Hub fortnightly newsletter and 33 out of the 55 respondents said they would like to be signed up.