Collaborating on data and cyber security Q&A

First edition - 20 May 2021

Webinar Q&A

This document provides answers to questions posed before and during the Better Security, Better Care webinar on Collaborating on data and cyber security held on 12 May 2021. It includes supplementary information to provide fuller responses and is not a verbatim record of the Q&A.

A recording of the webinar, presentation and this Q&A is available on the Digital Social Care website.

Better Security, Better Care and the DSPT

1. How long has DSPT being in existence and what has led to there being such a push recently for care providers to complete the toolkit?

The Data Security and Protection Toolkit (DSPT) has been in existence since 2018 where it replaced the NHS Information Governance (IG) Toolkit. Toolkit completion has been a contractual requirement for all health and care providers operating under an NHS Standard Contract since 2013, though this was rarely enforced. Adult Social Care providers have started to use the DSPT over the last few years. Care provider guidance has existed since 2017 and there has been a dedicated social care view of the Toolkit since the launch of the DSPT.

The DSPT has become increasingly valuable to care providers as more information is stored and shared digitally. Completion of the DSPT is a prerequisite for accessing many NHS shared records systems. As we are moving towards greater access to shared care records, using proxy access to order medications, and so on, there is an increased need for care providers to demonstrate that they are storing and sharing data safely by completing the DSPT.

The main benefits are that by using the DSPT, care providers can show that they comply with data protection legislation and the 10 Data Security Standards, and they can be more confident that they're resilient to cyber attacks and disruption to service.

2. What feedback are you getting about Better Security, Better Care and the DSPT?

Over the last year, we have updated and redesigned the DSPT so that it is more social care friendly. The latest version, which was developed in consultation with care providers, was launched in March 2021. It uses more social care provider language, rather than NHS. Providers have fed back that the revised version is much more user-friendly for them.

Care providers who have not visited the DSPT recently are encouraged to register and/or sign in. You can register online at https://www.dsptoolkit.nhs.uk/Account/Register

If you need support registering for the Toolkit, we have produced guidance on how to do this: Registering for the Data Security and Protection Toolkit

Regarding the Better Security, Better Care support programme, care providers said that, in isolation the DSPT can sometimes be intimidating. Local and national support is now available to help providers to complete the toolkit, and increase their confidence that what they are completing is correct. So far we have had positive feedback, with care providers reporting the support is helping them to feel more confident and dispelling some of the myths around data and cyber security.

3. Are the Standards Met via self-assessment or need external review and approval?

Yes, Standards Met is a self-assessment.

Digital Social Care is auditing a random selection of social care toolkit submissions this year. This is to assess the success of the changes to the Toolkit rather than as an external accreditation.

See guidance on Standards Met.

4. Can you expand on the deadline for the annual submission, you mentioned that not everything has to be submitted at once?

You can login to the DSPT and answer questions and answers autosave as you complete them which means that they will still be there when you log in next time and you don't have to answer all the questions at once. When you get to the point of having answered to the level required then you submit the completed answers. You should do this at least once a year, before the annual submission deadline (for 2020/21 this is 30 June 2021). Once you have published, you can return to your submission, make changes and updates and then publish again.

5. Does the next stage have to be completed by end of June? What happens if there is just too much info to get by end of June?

The deadline for completing the DSPT for the 2020/21 financial year is 30th June 2021. If you can't complete Standards Met by then, there is the option to publish at "Approaching

Standards" with an action plan for how you will answer the rest of the questions in the future. The DSPT will help you generate an action plan based on which questions you have not answered.

The Better Security, Better Care support programme will run through to mid-December 2021, so if care providers need support after 30th June because they can't reach this deadline, support will still be available.

6. The bring your own device (BYOD) requirements are quite a challenge to meet, any suggestions?

The most important thing is to understand what you are using BYOD for and what the risk are. Consider developing a BYOD policy and work with your staff to develop and communicate this.

Some of the requirements for organisations are also good for individuals such as ensure you have the ability to lock your screen or to remotely wipe your device if it is stolen.

If you have the budget, consider implementing a mobile device monitoring software. This is security software or a tool designed to help organizations secure, manage, and monitor mobile devices such as smartphones and tablets

But some simple checks can get you to Standards Met on the toolkit

Digital Social Care is currently developing additional guidance on this topic. If you register for Digital Social Care's newsletter we will let you know when it is available or contact:

- The Digital Social Care helpline: 0208 133 3430 or email help@digitalsocialcare.co.uk. 9am and 5pm Monday to Friday

Our current resources (as at May 2021) include:

- Protect Mobile Devices and Tablets – Digital Social Care
- Smart Phone Policy Template: BYOD – Digital Social Care (currently being updated)

Other useful resources:

- The Information Commissioner's Office guidance on BYOD.
- BYOD: Executive Summary - NCSC

Better Security, Better Care local support partner should be able to help you with specifics relating to your service. Ensure you know who they are and that you get in touch if you have further questions.

7. It says in the organisation search that my organisation is at Standards Met yet when I log in it says Standards not met. Can you please clarify?

It is likely that you reached Standards Met last year (2019/20) but that you have not published your assessment for this year (2020/21). You have until 30 June 2021 to publish for the year 2020/21.

For specific enquiries about how the DSPT is working for you, please contact the DSPT online help or their helpdesk:

DSPT Online Help

DSPT Helpdesk telephone: 0300 303 4034

Email: exeter.helpdesk@nhs.net

Please provide your ODS code or address when raising queries via email.

Or contact the Digital Social Care helpline with more general enquiries: 0208 133 3430 or email help@digitalsocialcare.co.uk. 9am and 5pm Monday to Friday

8. We have attained the "Standards Met" for the DSPT. We have the NHSmail, but have noticed no difference or experienced sharing care records with GP's. What would you advise we do to achieve this?

The national policy says that meeting Standards Met on the Data Security and Protection Toolkit is a prerequisite for all health and care providers to have access to NHS Patient Information or systems.

The current DSPT information standard says “All organisations that have access to NHS patient data and systems must use this Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.” This means that should a care provider achieve standards met, they will be able to take part in local shared records projects, proxy access to medication etc **where these projects are available**. Completing the Data Security and Protection Toolkit provides a firm foundation for starting conversations about information sharing. If using electronic care management systems, it is worth discussing with your supplier any integrations they have with NHS services that may be accessible upon completion of DSPT, for example GP Connect.

It would be the responsibility of local systems who are running these access to information pilots to advertise that these are running and to work with those providers who have completed the Toolkit to Standards Met. Shared care record platforms are expected to be available in every local area in England by September 2021, so they may not yet be available in your area but should in the coming months.

We suggest that you contact your local or regional organisation that is running the shared records system that you want to access. They will be responsible for confirming access. In most cases, this will be your Integrated Care System (ICS).

You may also want to make your Better Security, Better Care local support partner and regional coordinator aware of any ongoing issues that you may have. You can find their details on the Digital Social Care website.

Or you can contact the NHS Ageing Well Leads in your region.

9. If you have an HQ, but also other subsidiaries - do you do all the branches under HQ or do you advise individual subsidiaries?

It depends on the individual HQ/subsidiary model and size.

Please see the following documents:

- Registering for the DSPT

  This includes what ODS codes are and how to find yours, and guidance on what to do if your organisation has more than one site. This guidance is particularly useful for large multisite providers, domiciliary care organisations and providers offering multiple services as the process does vary depending on how your own organisation manages its data.

  You can also attend a webinar on how to register for the Toolkit. Find out more on our Events page.

- Guidance on multi-site organisations which are more than one legal entity.

You can also contact the Digital Social Care helpline. We can check the details and advise you on what to do.

You can contact the Digital Social Care helpline: 0208 133 3430 or email help@digitalsocialcare.co.uk. 9am and 5pm Monday to Friday

10. Do you have to log all data breaches through the DSPT?

Notifiable data breaches should be logged through the DSPT. The DSPT is linked in with the ICO so this will also fulfil the requirement to report data breaches to the ICO.

11. Is access to the systems free of charge to providers?

All support offered through the Better Security, Better Care support programme is free. It includes both national and local support. Access to the Data Security and Protection Toolkit is also free. https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/better-security-better-care/

Care Quality Commission and the DSPT

12. Do you know when/if using the DSPT will become a CQC compliance?

Using the DSPT is one of the best ways to provide evidence to CQC in relation to how care providers are storing and sharing information. It is not, however, currently mandatory for the DSPT to be used.

CQC is due to publish its five year strategy very shortly, and they will be developing a new inspection framework over the next 12 months. This will include considering how to identify the best evidence to support inspection and regulation. Therefore if the DSPT does become a requirement, it will not be before 2022.

CQC wants to work with system partners, including care providers, LAs and ICS, to support and encourage take up of the DSPT.

Care providers may also want to read CQC's interim guidance on What good looks like for digital records in adult social care.

13. Will the CQC strategy encourage providers to complete DSPT?

The CQC strategy will set out broad ambitions rather than specific details. CQC will be considering the future inspection framework including how do they identify best evidence. They want to help inspectors and care providers to identify that across all topics.

CQC wants to work with care providers and have conversations with about what does good look like in terms of digital and cyber security – what is best evidence that CQC should be prioritising, and does it need inspecting, or can CQC monitor it through other routes.

Register for CQC updates

Cyber Essentials

14. Will there any further funding available for support for Cyber Essentials Plus?

The National Cyber Security Centre (NCSC) is learning from the existing Cyber Essentials Plus services and the support provided to during COVID-19. Plans for the next steps of Cyber Essentials Plus+ are under review. No definite decisions have been made regarding funding.

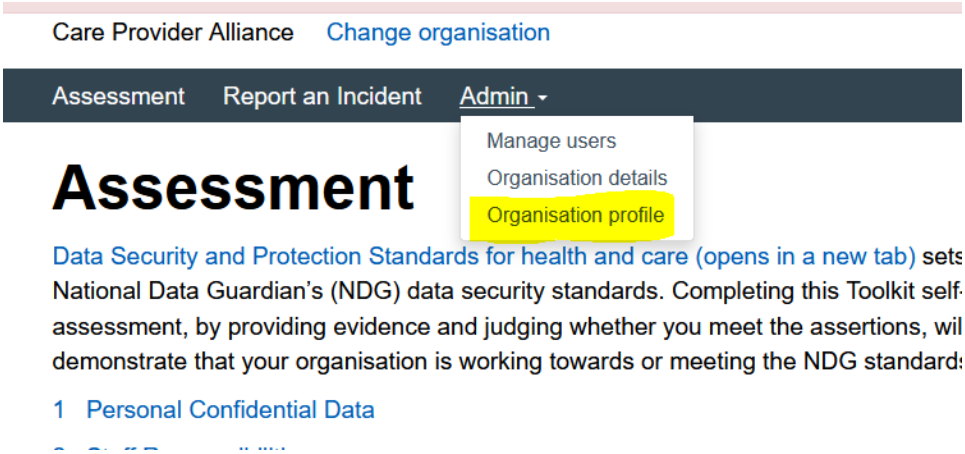
15. Does having Cyber Essentials Plus still act as a kind of passport for completion of some other mandatory elements of the DSPT?

Yes, if you have Cyber Essentials Plus certification it will auto-complete the relevant elements of the DSPT.

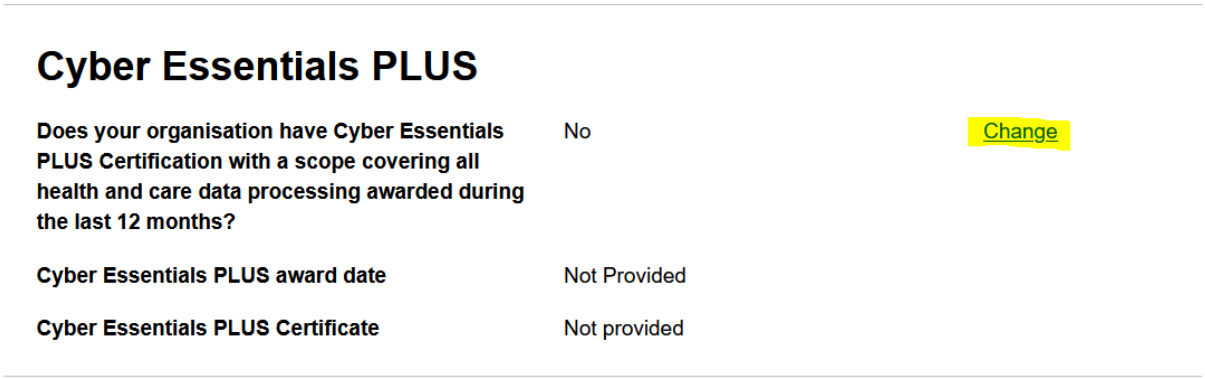
16. We have reached Cyber Essentials basic and plus. I was under the impression that by holding this certificate removed the need to complete some of the technical questions at the end of the toolkit. Is this the case as I can't find anything to state we have completed to Cyber Essential Plus?

Yes, that is the case. To confirm that you have completed Cyber Essentials Plus in the Data Security and Protection Toolkit, please complete the following steps within the DSPT.

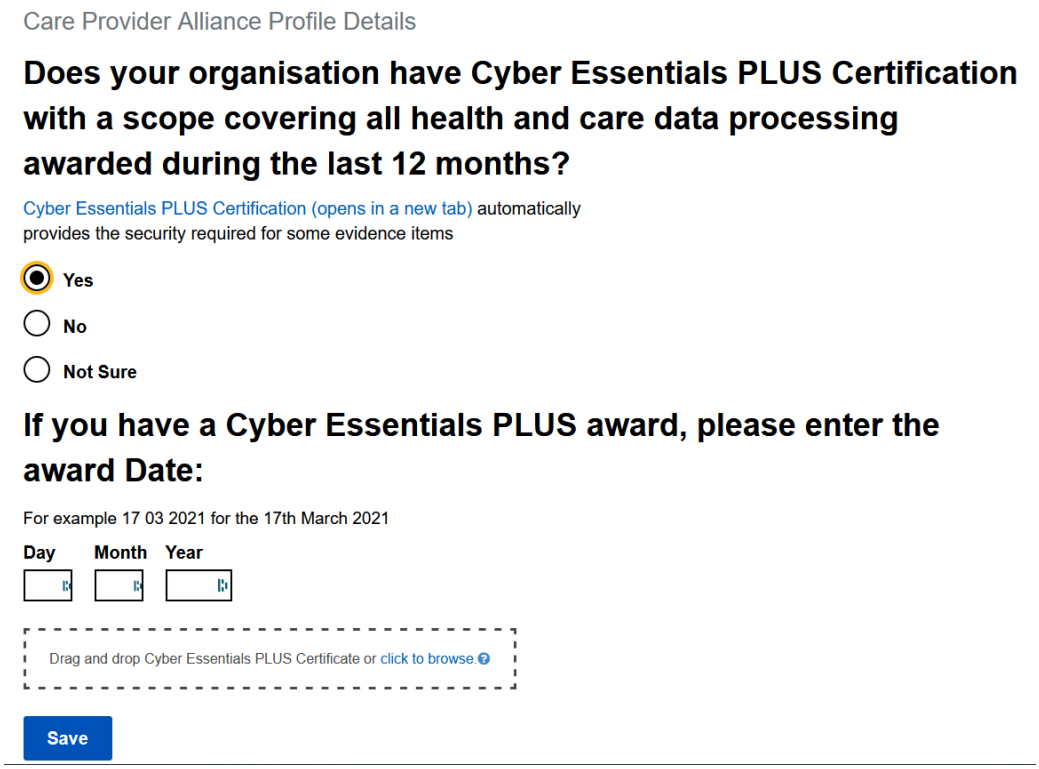
1. Click 'Admin' and then 'Organisation Profile'



2. Scroll to the section on Cyber Essentials and click 'Change'



3. Provide details of your Cyber Essentials Plus certification and click 'save'



If you're not able to do this, please do get in touch with either Digital Social Care or your Better Security, Better Care local support partner.

The Digital Social Care helpline: 0208 133 3430 or email help@digitalsocialcare.co.uk. 9am and 5pm Monday to Friday

Contracts and DSPT

17. Is there, or will there be guidance on reviewing contract clauses in relation to data security?

Local Government Association guidance includes suggested clauses for use by councils in their contracts with care providers.

DSPT is already a requirement within NHS contracts for care (see question below).

LGA and others within the Better Security, Better Care programme are working to ensure consistency across the sector including working with CCGs and ICSs.

18. Social care providers often need to act as data controllers in order to provide support but this is not always recognised in contracts. Can commissioners be advised to reconsider contract terms which state the provider is a processor only?

LGA and others are aware that there are issues within contracts about care providers' roles as data controller or data processer. LGA is taking this issue forward to consider this.

19. Are you looking at using contracts with commissioners and suppliers to ensure data security?

Contracts between commissioners and care providers, and care providers and data system suppliers should include data processing agreements, and privacy statements.

We recognise that there are many providers, commissioners and suppliers. Therefore it is complex. Digital Social Care and others are working to increase consistency. We do, for example, provide a series of templates for policies including guidance on what should be in care provider contracts with software suppliers:

- Template Policies
- Staff Guidance
- How to Document Your Data Processing
- Contract Guidance

CASPA is aware that not all care providers are requesting data system suppliers to provide clear data processing agreements. CASPA is working with suppliers to encourage system suppliers to proactively include this in contracts.

20. Are the clauses being built into the NHS Standard Contracts?

Yes, the relevant clauses in the NHS Standard Contract (https://www.england.nhs.uk/wp-content/uploads/2020/03/6-SF-GCs-100320.pdf) are below:

21.1 The Parties must comply with Data Protection Legislation, Data Guidance, the FOIA and the EIR, and must assist each other as necessary to enable each other to comply with these obligations.

21.2 The Provider must complete and publish an annual information governance assessment in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Services and the Provider's organisation type.

Access to NHS systems

21. If we get Standards Met, what do they need to do get access to NHS systems?

The national policy says that meeting Standards Met on the Data Security and Protection Toolkit is a prerequisite for all health and care providers to have access to NHS Patient Information or systems.

The current DSPT information standard says "All organisations that have access to NHS patient data and systems must use this Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly." This means that should a care provider achieve standards met, they will be able to take part in local shared

records projects, proxy access to medication etc **where these projects are available**. Completing the Data Security and Protection Toolkit is not a guarantee for access.

It would be the responsibility of local systems who are running these access to information pilots to advertise that these are running and to work with those providers who have completed the Toolkit to Standards Met. Shared care record platforms are expected to be available in every local area in England by September 2021, so they may not yet be available in your area but should in the coming months.

We suggest that you contact your local or regional organisation that is running the shared records system that you want to access. They will be responsible for confirming access. You may also want to make your Better Security, Better Care local support partner and regional coordinator aware of any ongoing issues that you may have. You can find their details on the Digital Social Care website.

The target is to have shared care records in place for primary care. The Joining Up Care programme is considering next steps for this – including how to involve social care in this.

Joining Up Care are rolling out advice and guidance on how to access GP records by proxy. They have trialled GP connect and wider access to summary care record application.

There will be more localised support for those initiatives over the next year, as Joining Up Care increases the roll out.

Data system suppliers and DSPT

22. Would a cyber security organisation be able to become a supplier with CASPA? We are working a range of NHS organisations helping them working towards both DSPT standards and CE+.

Have a look on Caspa's website https://caspa.care/ which sets out membership criteria. If you are working in social care space it is likely that you can become a member.

23. Would you expect a supplier of tech solutions to be registered with the DSPT and meeting Standards Met?

CASPA is encouraging all their members to reach Standards Met with DSPT. A lot of them already have DSPT as they already have NHS Contracts. A lot of members are able to support their own customers (ie care providers) in understanding DSPT and its requirements. CASPA are looking to make that uniform and would encourage all members to achieve that.

Products and systems

24. How to help adults with learning difficulties protect sensitive information that is necessary for accessing services such as email, online shopping accounts etc?

Please contact katie@digitalsocialcare.co.uk

25. Different Care Management Systems Providers use will it be possible to link those systems in the future? Instead of sharing emails with attachments?

The recent Busting Bureaucracy report outlined the ambition for all social care providers to have access to a digital social care record that can interoperate with a local Shared Care Record by 2024. NHSX's Digitising Social Care Records programme are proactively working in this space. You can find more information on their work here: https://www.nhsx.nhs.uk/blogs/support-digital-social-care-records/ or sign up for the Digital Social Care newsletter for more updates.

CASPA is working with INTEROpen to ensure that interoperability standards are promoted across its membership and that social care system suppliers are engaged in the conversations about advancing these interoperability standards. Many software suppliers are establishing integrations with other systems to enable 'systems to talk to each other' to reduce duplication for care providers and more seamless transfer of information to the right people at the right time.

26. What SIEM products do you recommend for Trusts?

(Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.)

NHS Trusts should visit NHS Digital's Data Security Centre Services Directions 2020 specification.

27. Comment on platform choices

To help social care and NHS organisations make the switch to Digital Social Care Records, NHSX has launched a new Dynamic Purchasing System (DPS), providing organisations with quicker and easier access to a list of quality-assured, accredited supplier solutions for digital social care records.

The accredited supplier list presents a marketplace where all suppliers have been assured, reassuring organisations that their preferred products have met a minimum set

of **requirements** around functionality, standards and interoperability to ensure they are compatible with both social care and NHS systems.

The DPS has just been launched (May 2021) and will develop over time.

Digital Social Care and CASPA are also publishing a template for software suppliers to complete in relation to the DSPT questions. Suppliers can then give this to their care provider clients for us in completing their DSPT self-assessment. The template will be available shortly.

Digital Social Care cannot endorse specific software suppliers or platforms, we are happy to speak to care providers and help with developing a strategy for how to choose and implement software in a way which works for you organisation.

We also produce success stories where we interview care homes, domiciliary care and supported living organisations about the software platforms they use and how they find them.

The National Care Forum's Hubble Project provides detailed case studies on three care services and how they are using digital telecare. It also provides advice, checklists and templates to support choosing and implementing technology enabled care.

Ransomware

28.What steps are being taken to protect against ransomware?

Ransomware is a type of malicious software (malware) which prevents you from accessing the information on your computer. The information can be locked, encrypted or stolen. You will then be contacted and asked to make a payment in cryptocurrency (e.g. BitCoin) to regain access to your information.

You should report this to Action Fraud either via their website or by calling 0300 123 2040.

If you need advice and support you can also report this to NCSC. The NCSC has also produced a list of things to do immediately if your computer is infected.

If the information affected includes personal information, e.g. details about staff or service users, then you might need to report this breach to the Information Commissioner's Office. If your organisation completes the Data Security and Protection Toolkit, you can report incidents within the Toolkit and it will help you decide if you need to report the cyberattack to the Information Commissioner.

Should I pay the ransom?

Paying the ransom does not guarantee that you will recover your files and it does not remove the malware from your computer. This also means you would be paying criminal gangs and that you are more likely to be targeted in the future.

What should I do to protect my organisation against ransomware?

There are lots of simple things you can do to protect yourself and your organisation against ransomware including regularly backing up your data, keeping your software up to date, and using antivirus and antimalware software. This advice is reflected in DSPT requirements.

We recommend using the NCSC guidance on mitigating malware and ransomware attacks.