DSPT information to assist care providers

Company name	Person Centred Software Ltd
Product name	Mobile Care Monitoring (MCM)

DSPT Number	Aproaching standards	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
1.2.1	Yes	Does your organisation have up to date policies in place for data protection and for data and cyber securityConfirm that your organisation has a policy or policies in place to cover: Data Protection, Data Quaility, Record Keeping, Data securityand, where relevant, network security.	Does your data processing agreement impact the care provider, if so please document your policy and the scope where it would affect the customer	We provide information to providers in our GDPR and DSPT toolkits and templates, easily accessible from with the MCM system.
1.4.1	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Please explain how your product manages and shares personal information	Yes (for Care information) All personal data shared by the MCM system is clearly visible within the application for all staff to see, as well as the date the DSA was agreed to and requires updated every 12 months to ensure the provider is fully aware of all data sharing from the MCM system
1.6.1	Yes	Does your organisation's data protection policy describe how you keep personal data safe and secure?	Please explain how your product keeps personal data secure	
1.6.4	Yes	What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately? Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question.	Do you manage customers mobile phones, if so please give your emplanation of how this impact your customers.	For the MCM system there is a sigining in and out book for the mobile devices. The devices returned to the charging station at the end of shift. (optional extra) PCS is contracted to provide MDM so that the devices can be wiped of personal data if lost.
1.6.5	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data? This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the Information Commissioner's Office (ICO	Please provide your DPIA templates	DPIA templates are available on request from Client Success for care providers using the MCM system.
1.6.6	No	If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	Does your product have any tools to manage BYOD devices? If so please document how this helps a customer	Our BYOD devices requires devices to be secured with either a password / biometric / pattern. The MCM system stores its data within an encrypted store that is only available to the authenticated owner of the device.
1.7.4	Yes	Does your organisation have a timetable which sets out how long you retain records for?	Please document your data retnention criteria	In line with Nice guidelines the MCM system set no limit on how long records can be retained for, however included in the standard pricing is 8 years records stored in PDF format and 3 years records stored as searcable data. Data transmitted to the NHS is retained within seperate systems for 30 years.
1.8.3		What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?	Please give the reverse of the question, explainined what they have implemented to mitigate risks, so the customer can rank them for all systems in use by them	
4.1.2	Yes	Does your organisation know who has access to personal and confidential data through its IT system(s)?	Please document how your product provides access control and audit of this information	The MCM system report "Worker Access Rights" can be used to provide an Audit of who has access to what personal data. All person data accessed with MCM is available by person accessed and the staff member that acced personal data for 8 yeras pior.

DSPT information to assist care providers

Company name	Person Centred Software Ltd
Product name	Mobile Care Monitoring (MCM)

DSPT Number	Aproaching standards	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
4.2.5	Yes	Does your organisation have a reliable way of removing or amending people’s access to IT systems when they leave or change roles?	If your product can assist in managing access rights then please explain here	In MCM If Dynamic IP Whitelist is enabled and NFC Location tag Scan for carer devices is enabled, then ex staff will automatically be denied access, more details can be found in the securiy documentation.
4.5.4	Yes	How does your organisation make sure that staff, directors, trustees and volunteers use good password practice? If your organisation has any It systems or computers it should provide advice for setting and managing passwords. Each person should havve thier .I;own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be "strong" i.e. hard to guess.	If your product can assist in managing password practice then please explain here	MCM has password polices available, as well as advanced NFC based two factor authentication.
6.1.5	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	Does your product have any tools to give visibility of who has accessed each individual data record?	
6.2.3	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions.	If you provide any of these devices then please explain any malware magement included on them.	If MCM is using devices provided by PCS have a simple process to update their security patches and reports to inform providers of devices which should not be used any more. PCS provide advice on mitigation procedures once a device has recived it's last security update.
7.1.2	No	Does your organisation have a business continuity plan that covers data and cyber security?	Please explain your business continuity plans for data and cyber security here.	
7.3.1	Yes	How does your organisation make sure that there are working backups of all important data and information? It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation’s back up systems work and how you have tested them.	Please document your data backup process.	MCM has data rentention and auditing built in to it as part of the service. In the event of DR recovery times are guanteed, all data is held in mutiple separate locations mutiple times.
7.3.4	No	Are backups routinely tested to make sure that data and information can be restored?	Please document your data backup process.	Backups are routinly restored and tested.
8.3.5	Yes	How does your organisation make sure that the latest software updates are downloaded and installed It is important that your organisation’s IT system (s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question.	Does your product have automated updates. If so, please document how this occurs, and how a customer can check which version they are running.	Yes, it is an integral part of the service along with user focused information to inform users of the updates. Generally two updates are delivered a day.
9.1.1	No	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?	Do you manage any WiFi routers for customers? If so, please explain how.	
9.6.2	No	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people)	Do you store data on customer devices then it is encrypted? If not then how would customers protect local data?	The MCM system ensures any personal data is stored in an encryped state or deleted upon exit.

DSPT information to assist care providers

Company name	Person Centred Software Ltd
Product name	Mobile Care Monitoring (MCM)

DSPT Number	**Aproaching standards**	**DSPT Question**	**Supplier information (CASPA)**	**Responses (only complete where relevant)**
10.1.2	No	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Please give contact details here	
10.2.1	Yes	Do your organisation's IT system suppliers have cyber security certification Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace	Please confirm if you have cyber security certification	Yes - it is not displayed on the web sites but is included within the security information provided to customers.
		Has your organisation completed the DSPT?	Have you completed the DSPT , if so where do you display this ?	Yes - this is published on the DSPT portal
		GDPR statement and contract with supplier	Please give a link to uyou GDPR statement, ideally in as plain English/easy to understand format as possible	The terms and contions for the MCM system are easily accessible from the marketing website and the MCM system, they have been written in plain english after extensive battles with lawyer to remove and simplify information.