DSPT information to assist care providers

Company name Name of your organisation
Product name Birdie

DSPT	Aproaching	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	Yes, Birdie has developed a comprehensive set of security policies covering a range of topics. These policies are updated frequently and shared with all employees. Policies are reviewed annually or prior to any major change.
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	See our DPA (https://birdie.care/dpa)
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	All data is password protected, access controlled, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes. All devices are protected by a leading enterprise mobility management technology. For detailed security information please see our security page.
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.	Discuss with care providers the arrangements they should consider to minimise the risks if mobile phones are lost or stolen and offer advise as necessary.	Where providers supply mobile devices to their teams, they often use a mobile-device-management (MDM) software to enhance security and improve the user experience for their staff. If you'd like recommendations for this, then we can support.
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	Care providers complete their own DPIAs, however may wish to discuss the supplier DPIA relevant to the technology that they are implementing to determine items such as data flows and data transfers.	Yes. DPIAs are performed prior to any new project where data processing is "likely to result in a high risk to the rights and freedoms of data subjects". We do this to make sure that we're always in control of our risks and we have procedures in place to mitigate them. Those DPIAs need to be reviewed and approvedby our DPO a senior member of the leadership team. We are also on hand to support our customers with their DPIAs if needed.
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	Wehn staff use their own decices, providers often use a mobile-device-management (MDM) software to enhance security. If you'd like recommendations for this, then we can support.
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	Birdie acts as a processor. The retention is set by the controller, the care provider. The retention period and archiving are the responsibility of the controller. As a processor we follow the controller's written instructions. At the end of the contract with the controller the data is returned to them or deleted and a certificate of deletion is provided. See the DPA for more details https://birdie.care/dpa.

DSPT information to assist care providers

Company name Name of your organisation
Product name Birdie

DSPT	Aproaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
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	* All employees complete Security and Awareness training annually as part of the commitment to NHS DSP toolkit. Our staff by whom the shared personal data is to be handled and processed are appropriately trained to do so in accordance with the Data Protection legislation. * Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All-access to personal confidential data on IT systems can be attributed to individuals and logged. The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. * All data sent to or from Birdie is encrypted in transit using 256-bit encryption. Our API and application endpoints are TLS/SSL only and score an "A" rating on Qualys SSL Labs' tests. We also encrypt data at rest using an industry-standard AES-256 encryption algorithm. Our dedicated infrastructure team is in charge of ensuring our platform is secure and available at all times. Once a year we engage third-party security experts to perform detailed penetration tests on the Birdie application and infrastructure (Last penetration test has been performed in November 2020 by KPMG).
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	Logging in to Birdie is secured by a one-time authentication link. We enable permission levels within the app to be set for care providers' staff so that only carers who've been invited by can access a client's information. These are defaulted to the most secure permission levels and can only be enabled by an affirmative action. More information on our security can be found here: https://www.birdie.care/security-by-design.
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	All our capabilities that may give carers or other users access to personal data are defaulted to 'off', and only switched on by the care provider, or upon their instruction.
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 .l;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	Logging in to Birdie is secured by a one-time authentication link removing the need to enter a username and password and making the app and webapp more secure.
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?	We had recordable near misses but nothing reportable to the ICO. Customers have been informed of the near misses voluntarily and no data were compromised. Post mortem have been conducted and mitigations action put in place.
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.	Where providers supply mobile devices to their teams, they often use a mobile-device-management (MDM) software to enhance security and improve the user experience for their staff. If you'd like recommendations for this, then we can support.

DSPT information to assist care providers

Company name Name of your organisation
Product name Birdie

DSPT	Aproaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
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.	We have a disaster recovery plan. The plan is reviewed and tested on a regular basis.
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.	Database backups of Birdie's production system are taken regularly and prior to any major upgrade or configuration change to Birdie's production environment. These backups allow, in the event of a disaster, the creation of a replica environment within a minimal period of time. Backups are stored in a different AWS environment.
7.3.4	No	Are backups routinely tested to make sure that data and information can be restored?	Please document your data backup process.	As part of the disaster recovery plan, backups restauration are tested on a regular basis.
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.	We ship upgrades on a regular basis to our web and mobile cloud-based applications. Users may be prompted to update their mobile applications from time to time, but the web application will never require users to run a 'system update'. We also continually monitor changes to regulations to ensure our software is compliant and handles those adequately. You can check which version of the Birdie app is installed on your mobile by opening your profile page.
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.	N/A
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)	Cloud systems are designed to reduce the need to hold any data locally, using API's to directly connect cloud based analysis and document system without the need to expose data to local storage risks. However, where the supplier includes provision of removable devices, these should be appropriately proetcted using encryption and /other technical measures.	N/A
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 for the provider to include in their supplier list	See list of approved subprocessors in the DPA (https://birdie.care/dpa)
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	Birdie has achieved Cyber Essentials certification.
		Has your organisation completed the DSPT?	Have you completed the DSPT , if so where do you display this ?	Yes. The information is displayed on our website and available on the NHS DSPT website (https://www.dsptoolkit.nhs.uk/OrganisationSearch/8KK24).
		GDPR statement and contract with supplier	Please give a link to your GDPR statement, ideally in as plain English/easy to understand format as possible	https://www.birdie.care/privacy-policy