CarePlanner eMAR
Data Protection Impact Assessment

This DPIA follows the process set out in the ICO DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The project concerns the development of an Electronic Medication Administration Record (eMAR) system, to be delivered via care workers' own mobile devices. The eMAR system comprises two key components: 1. An addition to our existing mobile application to give care workers access to medication information for the service users they support. 2. A new interface within our existing web application to allow the input of medical conditions, medication requirements and dosage frequency and administration routes. Traditional MAR sheets are paper-based records that remain in the service user's home, hindering the availability of the information they contain. An eMAR system makes the data instantly available to both the care worker (via the app) as well as the care agency (via the web application). Care workers can review the medications that they need to give, the dosages and administration requirements, and then confirm that the medication has, or hasn't been given, as well as any applicable reasons. A DPIA has been deemed necessary because the data being handled by the system is personal medical data, which is defined as a Special Category of data under the GDPR Article 9(1). It is also commonly data concerning vulnerable data subjects (recital 75).

Last updated: 17/09/18
Author: Mark Anslow
Classification: Private

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Customers of the CarePlanner system will input medication data into the web application, after obtaining the relevant **consent** or relying on another lawful basis. ↓ CarePlanner stores this data in a database that is encrypted at rest with 256bit encryption. ↓ Medication data is made available only to those care workers who are visiting the client that day, ensuring data minimisation. ↓ Medication data is transmitted to the app in an 256bit encrypted format, via an encrypted SSL connection, and stored at rest on the device in an encrypted format. ↓ New medication administration events are stored on the user's device (encrypted at rest), and then sent via an encrypted connection back to the CarePlanner system, where they are stored (again, encrypted at rest). ↓ Storage of the data continues until the service user's information is redacted (irreversible anonymised) or the customer leaves the platform.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The data being handled by the system is personal medical data, which is defined as a Special Category of data under the GDPR Article 9(1). It is also commonly data concerning vulnerable data subjects (recital 75). There are roughly 8,500 CQC registered home care agencies in the UK, providing support to around 500,000 people.[1] At optimistic levels of market penetration (25%), CarePlanner's eMAR solution could potentially end up processing data for around 125,000 individuals. Quantities of data are difficult to determine. On the assumptions that each service user has two rounds of medication each day, then, at the speculative market penetration levels given above, the system could be expected to handle circa 91 million records per year. Data retention periods are determined by CarePlanner customers. Typically, they are determined by the regulatory body (CQC), and may be up to six years. Individual customers may decide to reduce this period, and the Personal Data attached to the medication administration may be redacted at any time to allow reporting in aggregate on medication administration tasks without revealing personally identifiable information.

[1] https://www.cqc.org.uk/sites/default/files/20171123_stateofcare1617_report.pdf

When a customer leaves the CarePlanner platform, the data retention periods outlined in our Data Retention Schedule will apply.

CarePlanner sells internationally, primarily to English-speaking nations. However, 99% of our business currently remains with the British Isles. All data is processed and stored within the EU at all times, regardless of customer or client location.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

CarePlanner's relationship with the individuals about whom medication data is processed takes the form of a Data Processor, acting upon data collected and entered by our customers (the Data Controllers).

Our Agreement for Services clearly states (clause 9.1.1.2) that it is the Data Controller's responsibility to establish a Lawful Basis for processing Personal Data, which is in line with the precepts of the GDPR.

Data Controllers will need to carefully consider whether they are able to rely on the Vital Interests lawful basis for processing medication data. The ICO describes the Vital Interests basis as 'very limited in its scope', and although 'likely to be particularly relevant for emergency medical care', the regulator notes that 'it is less likely to be appropriate for medical care that is planned in advance'. This latter definition applies to nearly all medication giving in a domiciliary care environment.

The ICO also advises that 'you cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent'.

Domiciliary care agencies may also not be able to rely on GDPR Article 9(2)(h) following clarification in the Data Protection Act 2018 11(1), which allows processing of special categories of data only by 'a health professional or social work professional… [or] another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law'.

Finally, it is unlikely the relying on 'Performance of Contract' as a Lawful Basis for Processing will withstand scrutiny if the contract does not make specific reference to processing medication data.

All this means that it will be particularly important for Data Controllers who are planning to use the eMAR system to assure themselves that they have an appropriate Lawful Basis for processing medication data, and, if necessary, to obtain explicit consent from all service users capable of giving or withholding that consent before deploying the application, either as part of their standard service user contracts, or in a separate form.

It is worth noting, however, that in the majority of cases any eMAR system will replace an existing, paper-based system for recording medication administration. The data contained in a paper-based system will still be processed (for reporting purposes), which means that a domiciliary care agency whose staff are engaged in medication administration should have already obtained the necessary consents.

Customers will also need to ensure that service users are able to object to the processing of their medication data (or withdraw their consent), and that this is communicated to CarePlanner so that the necessary action can be taken.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The processing involved in eMAR falls under the following broad categories:

1. **Recording and sharing**: information about medication administration is collected at source and recorded using the mobile application; this is then made instantly available to administrators working in the agency office.
2. **Communicating changes**: information about medication changes is recorded by the agency office and then made instantly available to care workers in the field.
3. **Reminding/alerting**: warnings built in to both the web and mobile application will alert staff when medication hasn't been administered within a given time period.
4. **Profiling/alert**: warnings built in to the web application will potentially warn administrators when they detect medication trends; for example, *x* refused administrations of drug *y* within the last *z* days.

All these data processing functions are aimed at improving the accuracy, availability and completeness of the medication information, and ultimately improving standards of medication administration and service user safety. The data subjects themselves should enjoy greater reliability of medication administration and improved health/reduced morbidity as a result, as well as improved record-keeping for the benefit of other medical professionals who may be involved in the service user's care arrangements.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

As a Data Processor, it is not appropriate for Care Planner Ltd to consult directly with the Data Subjects themselves. Instead, we will consult with our Data Controllers to ascertain whether the system meets relevant data protection criteria, and whether it is fit for purpose.

This document will be circulated amongst beta testers of the eMAR system in order to make them aware of its data protection implications.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data

minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Our lawful basis for processing the data collected as part of the operation of the eMAR system is 'Performance of Contract'. As discussed above, our Data Controllers will need to establish their own lawful basis and record this appropriately. The Data Controllers should make sure that Data Subjects are fully informed as to the nature of the data that will be collected and processed, and Care Planner Ltd will provide necessary support in to Data Controllers. Data subjects' rights to portability and access are served by the provision of a Medication Administration Record report, which is exportable to common formats (PDF, CSV). Rights to rectification, erasure, objection and processing restriction can be accomplished either within the web application itself, or by a CarePlanner engineer. CarePlanner maintains a list of Sub-processors and ensures that these Sub-processors have appropriate security arrangements in place to uphold their data protection responsibilities, notably by signing Data Processing Agreements where appropriate, and reviewing privacy policies. Data Quality is addressed in our risk mitigation measure listed below. Data Minimisation and function creep-avoidance is part of a 'privacy by design' approach, which we aim to embed in our organisation through mandatory GDPR training. CarePlanner does not make international transfers of data.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm (Remote/Possible/Probable)**	**Severity of harm (Minimal/Significant/Sever)**	**Overall risk (Low/Medium/High)**
Data breach via mobile device: loss of data or unauthorised access	Possible	Significant	Medium
Data breach via web application: loss of data or unauthorised access	Possible	Significant	Medium
Unauthorised use via web application: access to data by an unauthorised member of staff	Possible	Significant	Medium
System failure (mobile application): mobile application fails to launch on device, or functionality is severely hampered	Possible	Minimal	Low
System failure (web application): web application fails to load, or functionality is severely hampered	Remote	Significant	Low
Data loss (mobile application): loss via device loss, damage or malfunction	Possible	Minimal	Low

Data loss (web application): loss via system crash or database damage	Remote	Significant	Low
Inadequate consent or other lawful basis obtained from data subject	Possible	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk (Eliminated/ Reduced/Accepted)	Residual risk (Low/Medium/High)	Measure approved (Yes/No)
Data breach via mobile device	Encryption at rest on mobile device; passcode on mobile device; passcode for app login; encrypted data transmission	Reduced	Low	Yes
Data breach via web application	Encryption at rest for web application database; encrypted backups; user login password policy	Reduced	Low	Yes
Unauthorised use (web application)	Permissions control system for eMAR module	Reduced	Low	Yes
System failure (mobile application)	QA process; Crashlytics monitoring service	Reduced	Low	Yes
System failure (web application)	QA process; New Relic monitoring; Disaster Recovery Plan	Reduced	Low	Yes
Data loss (mobile application)	Impossible to guard against handset loss (in terms of availability), but a lost handset will have an application lock code and an encrypted-at-rest database	Reduced	Low	Yes
Data loss (web application)	Full, live backups and Disaster Recovery Plan guard against this	Reduced	Low	Yes
Inadequate consent or other lawful basis obtained from data subject	Important for Data Controller to establish lawful basis. CarePlanner to include message in the eMAR system reminding about consent once it is established that this is the preferred basis.	Accepted	Medium	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Mark Anslow (Operations Director)	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Mark Anslow (Operations Director)	If accepting any residual high risk, consult the ICO before going ahead
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Mark Anslow (Head of Operations)	The DPO should also review ongoing compliance with DPIA