GDPR TOOLKIT

Making sense of the new regulation

Person Centred Software has produced this Toolkit to help our customers ensure the personal data you hold and process every day meets the new GDPR Regulation.

PERSON CENTRED SOFTWARE
MOBILE CARE MONITORING

Person Centred Software
1 Bell Court, Leapale Lane,
Guildford, Surrey, GU1 4LY

Table of Contents

Preparing for GDPR

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Act on 25th May 2018. The legislation has been updated to include previously unforeseen ways that data is now being used in the explosion of social media.

Our toolkit is designed to help our customers using Mobile Care Monitoring (MCM) prepare for the changes that GDPR brings.

Assessment

Data Protection Impact Assessment (DPIA) is used to document the personal data you hold and process, which is required for GDPR. Details of the data held in MCM including where it is stored, security measures and solution description is included. This will help you to incorporate it into the DPIA you are undertaking as well as corporate risk registers that you maintain.

Breach Notification

Should there be a data breach within the MCM application, notification processes are detailed to ensure the right people are made aware.

Privacy Policy

Our Privacy Policy for the use of MCM can be found at http://bit.ly/2BIEYRT

Features in MCM

MCM has tools for our customers to stay in control of their data as well as data flows/ processes and security to enhance GDPR compliance and mitigate data breach risk.

Overview of MCM

MCM plays a critical role in the effective management of residents' health and social care needs, helping social care providers and care staff support individuals in a safe, effective, responsive and caring environment.

Mobile Care Monitoring (MCM) – care planning and evidence recording for social care providers.

The MCM solution features **Monitor**, a web application to manage care planning processes, and a mobile solution called the **Care App**, which enables care staff to evidence the care and support provided contemporaneously, giving access to planned care.

Information processed in MCM is of a sensitive nature relating to health care needs of vulnerable individuals and therefore in scope for GDPR.

Data and information flows

MCM is used by care providers to hold care plans and record evidence of the care provided to service users and residents within their care. Care providers have a regulatory requirement to keep records related to the care and support of the individuals within their care and for whom they hold a duty to care.

Personal data

MCM is intended to hold personal data about the residents (service users) and staff within a home (location). For details about the data held, a description, purpose that it is being held for and the data flows, please refer to the following tables.

Devices

Person Centred Software currently provide Apple iPod Touch and Samsung Galaxy xCover 4 devices. Any data stored offline can only be accessed for a maximum 24 hours, after which re-validation with the servers must take place. This is to ensure maximum offline availability to the users within a care home.

Where Person Centred Software provide devices, each device is locked down. Apple iPod touch devices are secured using the Apple Configurator. Access is only permitted to the following functions:

- MCM Care App & Activities App
- Bluetooth Settings
- Wifi Settings
- Camera and Photo App
- Limited device settings
- Users are NOT able to install other apps, cannot browse the internet or change iCloud settings

Samsung Galaxy xCover 4 devices are locked down using Hexnode MDM. Access is only permitted to the following functions:

- Bluetooth Settings
- Wifi Settings
- Screen Brightness Settings
- MCM Care App
- Activities App

Where an xCover 4 is used, further security amendments can be made remotely using the Hexnode MDM Portal.

Where customers have deployed their own hardware/devices, then any lock-down or restrictions are configured by themselves or their chosen IT provider.

Service Users

Data Held	Description/ Purpose	Data Flow
File information to identify the individual	Name, Date of Birth, Location (Home), NHS number, NI Number and a profile picture are used to identify the person.	Data is controlled in Monitor and is sent to the Care App and Activities App for care staff to identify the person they are supporting.
Medical and Social history	Overview of a person's medical and social history that is relevant to supporting them in a social care environment, planning their care in line with their social needs, interests and any medical needs to be considered. This information may include any medical conditions that have been diagnosed.	Data is controlled in Monitor and is sent to the Care App and Activities App for care staff to provide an overview snapshot of the people they support.
DOLs and Capacity	Mental capacity assessments and documentation for any decisions made relating to capacity and consent.	Data controlled in Monitor and is incorporated in the care plan.
Risks to be aware of including any DNACPR or DoLS	Details of any risks that care staff should be aware of whenever supporting a person within their care.	Data controlled in Monitor and is sent to the Care App to provide important information at the point of care to the people support and individual on a daily basis.
Risk Assessments	A range of assessment tools capturing social and health risks or needs.	Data controlled in Monitor and is incorporated into the individuals care plan.
Care Needs & Planned Care	Agreed care plans in place are agreed between the provider and the resident and/or power of attorney. Care plans defining the needs, goals and actions required in each aspect of life, such as communication, personal care, medical and nutrition. Personal preferences are included in planned care actions as well as when actions are performed on an ad hoc basis.	Care plans are created and reviewed in Monitor and available to care staff through the Care App when required. Planned care actions are managed through Monitor and presented on the Care App to inform staff of any actions that need to be carried out.
Care Notes	Evidence of care provided details the type of action and notes of any observations and interventions provided.	Care notes are recorded via the Care App and the Activities App. Recorded by Care Staff who are providing support.
Charts	Medical observation charts, including weight, blood pressure, pulse as required to monitor a service user's health. Other charts used to manage and monitor needs, such as personal hygiene, activities, re-positioning, night checks and nutrition.	Charts are generated from the data captured in the Care App and are presented in Monitor for management and visibility of important information relating to health and care needs.
Contacts	Contact details for friends and family, health care professionals and other contacts who are involved in the care and support of an individual.	Contacts are managed in Monitor with emergency contact information also available on the Care App.
Photos	Care staff can take photos of residents for activities and wound management or to capture moments in the care home.	Using the Care App, photos are directly stored in the secure cloud. Authorised users can control the access to the photos uploaded to the 'photo stream', ensuring only the appropriate people can access the photos.

How is Data obtained?

When a service user is created in MCM, the file information usually provided by the service user or the representatives during the admission process and entered by staff at the care home / service. On-going care planning and evidence of care is entered by the staff supporting the individual.

Integration with other Data Processors

Where the care provider is moving their data from a previous software vendor, data may be 'migrated' from a 3rd party solution when agreed by the Data Controller.

Integration with any Third-Party Applications

Using the secure Application Programming Interfaces (APIs) in MCM, Data Controllers can set up an API key linked to an authorised user record which enables data to be integrated to other software solutions. Person Centred Software will not share personal data with 3rd parties unless there is a lawful reason or legal requirement (such as criminal prosecution).

Policy – Retention of Data

Care providers are required to keep records of service users care plans and evidence of care provided. Service users' records can be archived in MCM once they no longer receive care from a provider to restrict further processing. Adult services will be retained in MCM for 8 years, in line with the recommended guidelines set out by the Information Governance Alliance.

Policy – Data Correction

As MCM holds evidence related to the care provided to service users and would be required in case of any legislative or regulatory action against a care provider, care notes cannot be deleted from MCM. Subject to access rights, care notes can be marked as 'Void' within 3 months of entry, so that information held is accurate. MCM does permits the correction of care notes up to 2 months, but requires confirmation from the original author, and audit history is retained for any corrections made. Records will be retained in line with recommended data retention schedules for the type of service user being supported.

Users/Staff/Worker Records

Care staff and system users are held in MCM to manage user access, identify workers as part of the evidence of care, and to hold limited contact information.

Data held	Description/Purpose	Data Flow
File information to identify the individual	Name, Date of Birth, Email address, Location of work (Home), NHS number, NI Number and a profile picture are used to identify the person.	Data about the worker is held in Monitor.
Pay rates	Hourly rate of pay is held to calculate the cost of care provided.	Data about the worker's pay rate is held in Monitor.
Contacts	Contact details for friends and family and other contacts who might need to be contacted in relation to the worker.	Contacts are managed and viewed in Monitor.

Security

Information is accessible to care staff with valid logon to MCM whose user account has access to the community in which the service user is set up in MCM. User accounts are managed by the Data Controller.

We frequently conduct 'Penetration testing' on our software and infrastructure by a Check Registered third party to certify that data is held securely. This is supplement to our hosting company's own security measures.

Where data is held?

MCM is a SaaS (Software as a Service) solution and is hosted on the Microsoft Azure platform. Individuals' data is segregated by the organisation who is responsible for the individual / where they are receiving care, data is further segregated by the service to which they are living in or receiving care from.

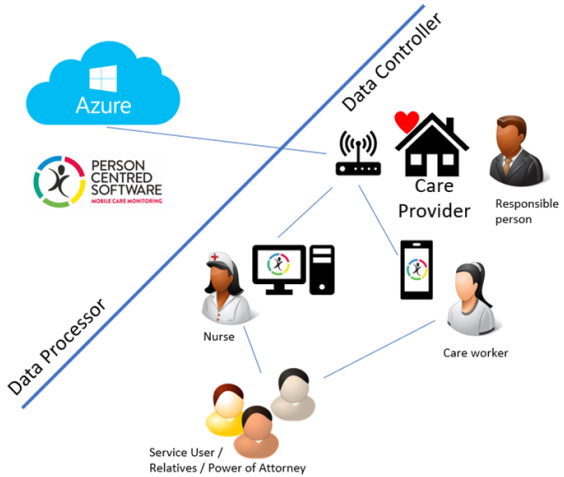
Server infrastructure

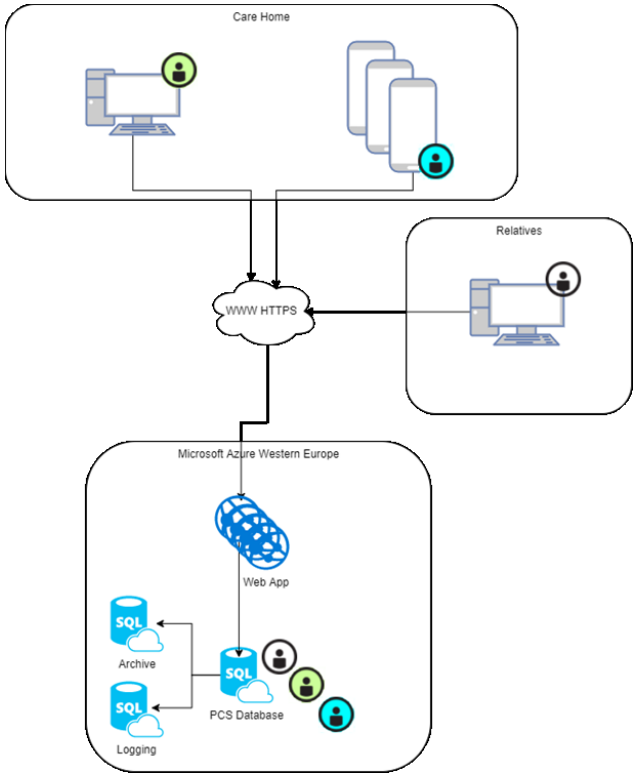
The Person Centred Software servers are hosted by Microsoft in their Azure cloud service. The data is stored within the EU to ensure that GDPR and data protection security standards are not breached.

Data on the servers is both backed up and replicated within the EU data centre network. To achieve this, we use the Microsoft Azure Geo Replication service.

The Azure service is always fully up to date with the latest security patches and virus definition updates, ensuring further compliance with GDPR data protection legislation.

Access to the MCM application is through a web browser using Secure Socket Layer (SSL) only.





Risk Register/ Privacy Solutions

Risk	Solution(s)	Result: is the risk eliminated, reduced or accepted?	Evaluation
Unauthorised access through incorrect permissions granted	User access to individuals' information is restricted by user name and password that are controlled by the Data Controllers/Customer. Password renewal policies can be set by the organisation.	Risk is reduced to an acceptable level. A small risk remains where individuals' access rights are incorrectly allocated, but this would remain within the same Organisation.	Users require individual user name, password and access rights for the safe use of MCM.
Printed records are not handled securely	MCM promotes a paperless working environment within the care setting to avoid the systematic printing of personal data. However, there may be occasions where printing of information is required, such as (but not limited to); hospital pack; care plan documentation; care note reports; and file information.	This risk is accepted, and a data breach is no more likely than using paper documentation.	The need and benefit to the individual to provide care plan data to other Health Care Professionals (including emergency services and hospitals) as well as any relatives with Power of Attorney would outweigh the potential risks to the individual.
Inappropriate data disclosure to unauthorised 3rd parties.	Where other 3rd parties, such as inspectors or Health Care Professionals are involved in an individual's care, then read only access can be granted as appropriate, but only to the required individual.	Risk is reduced to a minimal level.	Access is only granted where it is appropriate. This is controlled by users of MCM with adequate permissions.
Incorrect/inaccurate data	Personal data can be corrected by the authorised user within Monitor. Where incorrect evidence of care is recorded, due to the nature of the data captured, care notes can be corrected within 2 months of entry or voided within 3 months of creation.	Standard processes and procedures should reduce the risk of holding incorrect data. Changes are audited and data such as care plans and care need cannot be deleted.	Data entry mistakes can be made no matter what solution is being used. MCM is designed to capture information simply and easily by care staff. Care notes are regularly reviewed by staff with correction or void processes in place to enable errors to be corrected.
Data is unlawfully accessed by third party	MCM is hosted on the Microsoft Azure platform which adheres to the highest industry standards. In addition to this, Person Centred Software carry out penetration testing conducted by a third party specialist.	The MCM platform is hosted on industry leading platform to reduce risk to acceptable levels.	MCM is sufficiently secure for the information held about individuals.
MCM is used in ways un-intended	Training, in-app help, support desk and a purpose built solution is provided by Person Centred Software Ltd.	A small risk of a human error or a customer's decision to record information into MCM that it was not designed for.	MCM is a trusted solution in use at over 500 care provider locations.
Please add any other risks you identify or wish to record			

Data Breach Information

Person Centred Software treat the security and privacy of the personal data we hold on behalf of our customers and the people they support very seriously. As **Data Processors,** GDPR requires us to have a process in place to notify customers (**Data Controllers)** of any data breach that occurs with the data we hold.

What is a breach of personal data?

> *The ICO define this as: "A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data."*

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-breaches/

If a personal data breach occurs as a result of our software or processes and practices, then we will notify the **'Responsible person(s)'** recorded within Mobile Care Monitoring (MCM).

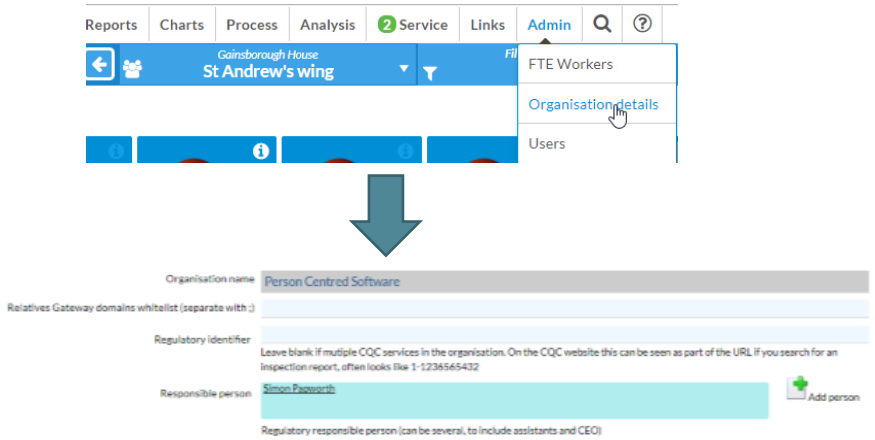
*PCS will aim to notify customers within **24 hours** of becoming aware of the data breach.*

Responsible Person

To view/add or remove the specified responsible person; go to the 'Admin' menu and then select 'Organisation details'.

You'll then see a section where you can add a person (or multiple people) for the Organisation.

You can also set a responsible person on the **Community details** page (Use the community that has been set up to represent the Location)



Note: You can also add Responsible people for each location. This is set up in the Community details for the community that has been set up to represent the home / CQC service.

Data Breach Notification Process

Data Controller: under GDRP, Data Controllers are obliged to notify the supervisory body (ICO – Information Commissioners Office in the case of the U.K.) within 72 hours of being notified about a data breach.

Data Processors: As per obligations under GDPR; Person Centred Software will notify the responsible person(s) for each organisation in the event of Person Centred Software becoming aware of a notifiable data breach of the personal data they control. Notifications of a data breach will include the date, summary of incident, nature and content of the personal data, any potential effects on individuals, measures/actions taken to address the breach, and how our customers can mitigate any possible adverse effects.

Document Sign-Off

Each DPIA should be signed off by the people within your organisation who are responsible for the control of personal data.

Exceeding GDPR

Next Steps for MCM

In addition to the secure data storage and transmission processes, the MCM solution enables organisations and users to meet and **exceed** GDPR requirements.

The current solution enables compliance to GDPR, but we believe in going beyond just the necessary and provide a solution that enables our customers to more efficiently manage their data security.

In time for GDPR, by May 2018 , MCM solution will be updated to feature:

- Enhancements to password management process
- User access and rights matrix—to see who has access to each community and what access privileges they have been granted
- Record access audit—Track which records a user has had access to per day, audit who has access a particular record and log access from any third party approved APIs
- Device unenrolment —Organisations will be able to remove devices from those that are enrolled for use

Other things to remember:

The Care App can be configured by each Location to only permit access from specified IP address ranges, so that when used outside of the local network the device will not display any data.

01483 604108

care@personcentredsoftware.com

www.personcentredsoftware.com

PERSON CENTRED SOFTWARE

MOBILE CARE MONITORING