



GDPR Toolkit

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.

Overview of mCare

mCare 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. Developed specifically for the industry by Person Centred Software in 2013; it has become the leading software solution for care homes.

mCare – care planning and evidence recording for social care providers.

The mCare 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 MCARE is of a sensitive nature relating to health care needs of vulnerable individuals and therefore in scope for GDPR.

Data and Information Flows

mCare 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

mCare 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.

Preparing for GDPR

The EU General Data Protection Regulation (GDPR) came into effect on the 25th May 2018. The UK updated the Data Protection Act to reflect GDPR and incorporate it into its own legislation. The legislation has been updated to include previously unforeseen ways that data is now being used in the explosion of social media and digital solutions.

Our toolkit is designed to help our customers using MCare to meet GDPR and the Data Protection Act 2018, but this toolkit is by no means exhaustive and we recommend seeking third party legal advice. Further information is available from the NHS DSP Toolkit and Cyber Essentials from the National Cyber Security Centre.

GDPR Definitions

Throughout this document, specific terminology relating to GDPR definitions will be used; these key definitions taken from the Information Commissioner's Office website (ICO) are:

Data Controller - A controller determines the purposes and means of processing personal data. Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data; for example, this would be the Care Provider or Care Home.

Data Processor - A processor is responsible for processing personal data on behalf of a controller. Processors act on behalf of, and only on the instructions of, the relevant controller. In this instance, this is Person Centred Software.

For more information, please see: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulationgdpr/key-definitions/>

Your Responsibilities

Data Impact Assessment (DPIA)



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 MCARE 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.



mCare 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.

Breach Notifications



Within 72 hours of a data breach, you have a responsibility to inform the ICO that a breach has occurred. A data breach could occur within your Organisation, or it could be a mistake that Person Centered Software makes in processing your data. Should there be a data breach within the mCare application, notification processes are detailed to ensure the right people are made aware.

Privacy Policy



If you don't have a privacy statement, a good template is <https://www.digitalsocialcare.co.uk/resource/privacy-notice-template/>
Our Privacy Policy for the use of mCare can be found at <https://care.personcentredsoftware.com/mCare/caredeliverydevice/privacy>

Comply with the Data Protection Act 2018 and UK GDPR

Why Secure Devices are Important

You and your organisation has a responsibility to ensure that your data is kept safe from unauthorised access.

The Care App can be run on most recent Android (recommended) and iOS devices. Where **Person Centred Software** provide devices, each device is locked down as described below:

- a) Apple iPod touch devices are secured using the Apple Configurator. Access is only permitted to the following functions:
 - mCare Care 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
- b) Android devices are locked down using Mobile Device Management (MDM)*. Access is only permitted to the following functions:
 - Bluetooth Settings
 - Wifi Settings
 - Screen Brightness Settings
 - mCare Care App

Mobile Device Management (MDM)

Mobile devices can be very powerful and enable people to carry out multiple functions, with access to a wealth of content and applications. However, when deployed in a Care Home environment they are primarily a tool to support the Carers in their role; but without adequate control mobile devices can become a distraction and a security risk. With Person Centred Software's MDM service, it gives you the flexibility to deploy just the Care App or add to your Organisation's profile a number of useful apps for example, a third-party call bell monitor.

Person Centred Software's MDM will also enable the estate of devices to be managed remotely, to update the operating system, add and remove Apps on the devices at request and also ensures devices can be de-activated and enrolled as needed. As the MDM service is managed by Person Centred Software we can ensure our services are compatible with the devices, for the current and future product.

Where **customers** have deployed their own hardware/devices, then any lock-down or restrictions are configured by themselves or their chosen IT provider. Any data stored offline on the Care App 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.

Devices and Security Patches

Software security is becoming one of the biggest focuses in the mobile world. Larger manufacturers have a longer-term commitment to their customer base, and Google have stipulated that manufacturers who ship over 100,000 devices must support software and security updates for a minimum of 2 years from the device release date to remain an accredited google certified device. Cheaper devices will not fall into this category and the responsibility of finding and applying software updates to those devices will be with the end user, not the manufacturer. Before purchasing a device, your Organisation must ensure you know when software patches will end.

The National Cyber Security centre have a very good article on migrating away from obsolete software - <https://www.ncsc.gov.uk/guidance/obsolete-platforms-security-guidance#Migrateawayfromobsoletesoftware>; it is worth noting that this affects mobiles as well as PCs.

What type of data is Held in mCare?

The following tables outline the types of data held in MCARE for Service Users and Staff records.

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.

Users / Staff / Worker Records

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.

Relatives Gateway

The Relatives Gateway is an optional component to mCare. Organisations can provide friends/relatives or even the resident themselves access to a portal. The portal provides the ability to share information. The information made available on the Relatives Gateway depends on which components are made available by the Organisation/Care Provider as well as on an individual contact by contact basis.

The Components that an Organisation can make available (or disable) on the Relatives gateway are described below.

Portrait	The profile picture of the residents
Happiness Chart	highlights the resident's level of happiness on a given day, over the last week
Messenger	A way to share messages and photos to/from the care home, care staff (those using Monitor) and other connections who have access to the relative via the Gateway
Gallery	View photos that have been shared on the gateway
Care summary	Table showing number of interactions, hours of care delivered and other summary information over a 4-week period compared to up to a year ago
Plan of care to be provided	The daily plan shows a) picture of resident b) DOB c) risk to be aware of d) DNACPR status e) Likes to talk about f) medical and social history g) height/weight and BMI h) All of the planned care actions
Daily care provided	Each care note recorded shown by time of day (morning, afternoon, evening and night). Actual time and user details are not shown
Care notes story	Summary of care notes compiled into a paragraph. Shown by time of day (morning, afternoon, evening and night). Actual time and user details are not shown
Care notes chart	Each care note recorded shown by time of day (morning, afternoon, evening and night). Actual time and user details are not shown. Report can be filtered by user
Care hours per ADL chart	Average number of care notes entered per day over last 4 months
Care notes per ADL chart	Care notes hours per day
Care plan document	The full care plan for the resident and the ability to record consent (NB: only available to contacts with Power of Attorney for Welfare)
Activities chart	Chart showing activities participated in over last 28 days
Fluid chart	Fluid summary of offered/consumed in last 7 days
Hygiene Chart	Chart showing what personal care has been provided over last 28 days

Once the Relatives Gateway has been enabled by a provider, then when a contact is set up, they can be given access to any of the available components.

It is the providers responsibility to ensure that the appropriate legal grounds or consent have been obtained and documented before giving relatives/residents contacts access to their records.

How is Data Obtained?

When a service user is created in mCare, 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 mCare, 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 mCare once they no longer receive care from a provider to restrict further processing. Adult services will be retained in mCare for 8 years, in line with the recommended guidelines set out by the Information Governance Alliance.

Policy – Data Correction

As mCare 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 mCare. Subject to access rights, care notes can be marked as 'Void' within 3 months of entry, so that information held is accurate. mCare 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.

Security

Information is accessible to care staff with valid logon to mCare, whose user account has access to the community in which the service user is set up in mCare; 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.

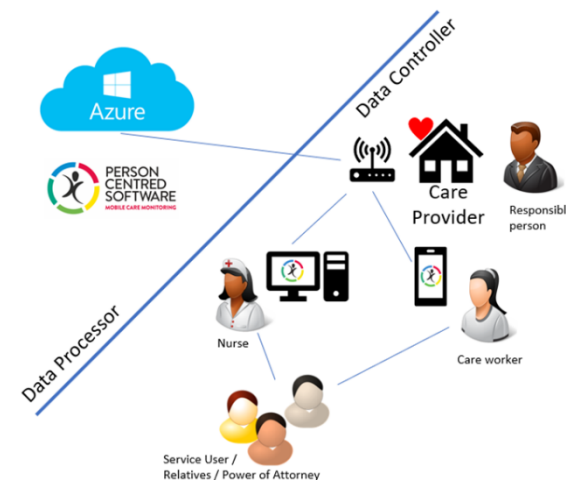
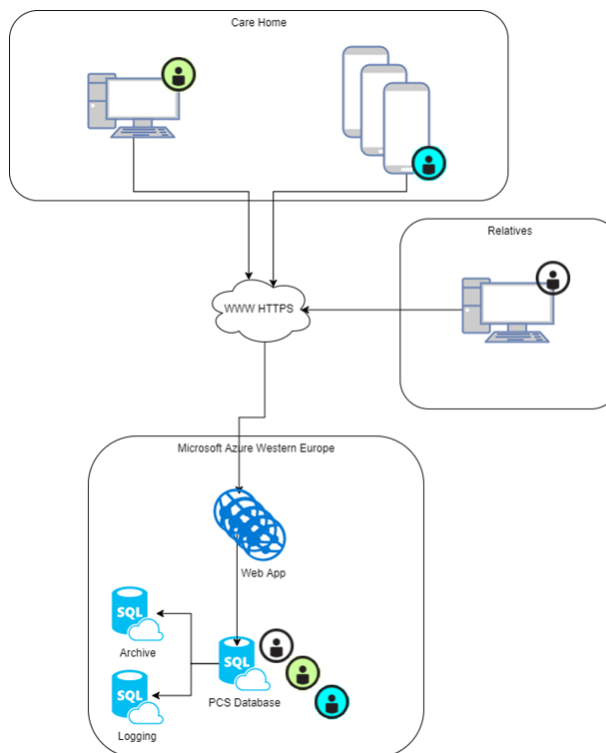
Where is data held?

mCare 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 EEA (European Economic Area) to ensure that GDPR and data protection security standards are not breached. Data on these servers are both backed up and replicated to a secondary region within the EEA. To achieve this, we use the Microsoft Azure Geo Replication service, this ensures that data is replicated both within a region and across regions. 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 mCare application is through a web browser using Transport Layer Security (TLS) only.



Person Centred Software follow the NHS guidance on cloud services. Per this guidance, PCS “Only use Cloud infrastructures to store and process data that are physically located within the European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.”

Note: This is guidance from the **Cloud Security Good Practice Guide**.

Where Users Can Access Data From?

The Monitor component of mCare is a website application and is by default able to be accessed from anywhere with internet access. Whilst GDPR does not dictate any restrictions of where information can be accessed from, it concerns itself more with who and the legitimacy of access; providers should consider putting measures in place to control access based on the location of a user when accessing data. This is not necessarily straight forward, as there may be good reasons for accessing data from a location other than the care home itself (e.g. hospital admissions, activities outside of the home, manager or responsible person escalation whilst they are outside the care home facility, head office, regional management etc.).

The Care App and Monitor can be configured by each Location to only permit access from specified IP address ranges, so that when used outside of the local network no data will be displayed.

Support Access

To be able to support providers with the use of mCare and any troubleshooting required, support staff at Person Centred Software may need to 'impersonate' users (this effectively means being able to use/see the system as if they were the user). Audit access logs show if a user was being impersonated. Person Centred Software staff will ask permission from users when they require the need to impersonate to provide necessary support.

Example Risk Register / Privacy Solutions

This document is designed to help care providers understand the data protection risks associated with mCare but this document is by no means exhaustive as working practices will differ between providers. We recommended providers use the below example risk register and create/add them to their own corporate risk registers - seeking third party legal advice when necessary.

Risk	Details	Solution(s)	Result: is the risk eliminated, reduced, or accepted?	Evaluation
Unauthorised access through incorrect permissions granted	<p>When a User Account is created by a person with the appropriate permission levels; it is their responsibility to ensure that the correct 'Access rights' are granted and the User account and that the worker(and associated User Account) are allocated to the correct Communities in MCARE.</p> <p>If this is not managed correctly; then a user may be given incorrect access to personal data for residents or staff, they are not entitled to see.</p>	<p>Each home using mCare will need to have a person(s) who responsible for the creation and maintenance of user records. Make sure staff at the home know who's responsible.</p> <p>Once staff, user and service user information has been set up; person(s) responsible for user access to mCare should run the Worker access rights report to check that the correct levels of access have been granted.</p> <p>Periodically (at least once a month or when there has been a change of any key personal/responsible people) check the Worker access rights report.</p> <p>When user records are created, you'll need to allocate them a temporary password (PLEASE NOTE: through the staff import process user are set up and allocated a standard password). We suggest that you immediately get the user to log-in and ask to change their password to something only they know and then ask them to confirm they have changed it from the temporary password.</p>	<p>Risk is reduced to an acceptable level.</p> <p>A small risk remains where individuals' access rights are incorrectly allocated.</p>	<p>This risk is mostly down to user error or where no internal process has been created or followed and is the responsibility of the data controller / care provider to ensure checks are made.</p>

		<p>Providers should have an operational policy in regard to using the Care App and Monitor to outline safe working practices.</p> <p>The Care provider is required to ensure they have a process for managing staff and user records as soon as personal data has been entered mCare.</p> <p>Person Centred Software support staff will NOT manage user's access to mCare and will only provide instructions to do so.</p>		
Printed records are not handled securely	<p>mCare promotes a paperless working environment within the care setting to avoid the systematic printing of personal data.</p> <p>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.</p>	<p>Only ever print information where necessary and ensure that all staff have been adequately trained in safe methods of data handling for both digital and paper formats. This should form part of your mandatory training and induction processes for all staff using mCare.</p> <p>Printed information from mCare is solely the responsibility of the data controller/provider to handle securely.</p> <p>Never leave paper containing personally identifiable data in an insecure location.</p>	<p>This risk is accepted and can be reduced by using electronic solutions and only printing information when necessary.</p>	<p>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.</p>
Inappropriate data disclosure to unauthorised 3rd parties.	<p>Where other 3rd parties, such as inspectors or Health Care Professionals are involved in an individual's care, then read only access may be required.</p>	<p>Specific Communities, User Accounts and Read-only access rights can be set up by the care provider in order to give authorised 3rd parties with legitimate need to access records (for example where a CQC inspector is inspecting a residents file).</p> <p>Never share user account details with anybody else and never log-in to mCare and leave the application logged-in for other people to use your credentials.</p>	<p>Risk is reduced to a minimal level.</p>	<p>This is controlled by users of mCare with adequate permissions.</p>

Incorrect/inaccurate data	<p>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.</p>	<p>Care notes should be reviewed on a regular basis. If errors are identified, then the care note correction process or voiding processes should be used to correct the error.</p> <p>Staff should advise of any error to the appropriate person in their home of any error or incorrect data immediately and either corrected or voided where applicable. Note: Care notes can be corrected within 2 months of entry or voided within 3 months of creation.</p> <p>Other data can be amended accordingly with changes made being audited.</p> <p>It is good practice to review the Audit changes report and Care planning audit to help identify changes made</p>	<p>Standard processes and procedures should reduce the risk of holding incorrect data.</p>	<p>Data entry mistakes can be made no matter what solution is being used.</p> <p>MCARE is designed to capture information simply and easily by care staff.</p>
Data is unlawfully accessed by third parties	<p>mCare is a cloud-based solution and unlike the majority of other applications, can have its access limited to specific locations.</p> <p>Cyber threats are always a threat to any business.</p>	<p>mCare is hosted on the Microsoft Azure platform which adheres to the highest industry standards.</p> <p>Person Centred Software carry out penetration testing conducted by a third-party specialist twice a year as minimum OR where a significant change in infrastructure is made.</p> <p>It is good practice for the care provider to review the access audit reports to help identify any suspicious activity.</p>	<p>The mCare platform is hosted on industry leading platform to reduce risk to acceptable levels.</p>	<p>mCare is sufficiently secure for the information held about individuals.</p>
mCare is used in ways unintended	<p>Training, in-app help, support desk and a purpose-built solution is provided by Person Centred Software Ltd.</p>	<p>The care provider should ensure that all staff use the Care App and Monitor are sufficiently trained in how to use mCare.</p> <p>Provision should be made for ongoing training and keeping staff up to date with any changes to the system and new features.</p>	<p>A small risk of a human error or a customer's decision to record information into MCARE that it was not designed for.</p>	<p>mCare is a market leading solution that takes data security very seriously and have designed a solution that is simple to use by workers with varying levels of IT literacy.</p>

		<p>Providers should have an operational policy in regard to using the Care App and Monitor to outline safe working practices.</p> <p>Enterprise help content can be created to provide specific organisation level guidance on how to use features/pages in Monitor</p>		
Malicious use of the system	<p>If someone wishing to act criminally has access to the system unlawfully through using their previous credentials or using someone else's where credentials have been compromised, there is a risk of malicious activity,</p>	<p>Use the Password change policy to ensure that users change their password frequently</p> <p>As soon as you go as you have entered personal data into mCare and set up staff records ensure that all staff go in and use the Change password feature on the Care App or via Monitor to change their password from any allocated password. Staff should be trained on password security standards. Where user's login accounts are valid emails, this can also be don't via the Forgotten password process</p> <p>Ensure that only authorised staff are given the user access right to "Manage Staff and run staff reports"; as user with this right can view staff detail and change user access rights.</p> <p>If staff are suspended from duties (for example where there is a disciplinary procedure in progress) then it is advisable to remove the User account from the staff record until the outcome of any disciplinary procedure is known.</p> <p>Check audit access logs frequently to help identify any suspicious access</p>	<p>Risk reduced to as minimal as possible with potential risks accepted by the care provider</p>	<p>Providers must manage and monitor access.</p>

		Check the Worker Access Rights Report to ensure that passwords are being changed frequently		
Inappropriate access to data outside of where reasonably expected	<p>MCARE is designed to be able to be accessed from anywhere with internet access as this provides the greatest capability, however users with valid credentials could access data from anywhere in the world at any time. This may lead to inappropriate access and increased risk of data being breached.</p> <p>Whilst GDPR does not dictate specifically any restrictions of where information can be accessed from, it concerns itself more with who has and the legitimacy of access; providers should consider putting measures in place to control access based on the location of a user when accessing data.</p>	<p>Organisations should consider implementing IP address restrictions to Monitor and/or the Care App.</p> <p>The Care App can also be secured further using NFC Location Tags that require users to scan a physical tag to enable them to log into the Care App.</p> <p>Providers must weigh up the benefits/costs of the option of restricting access to specific IP addresses vs. enabling staff to work from anywhere.</p> <p>Check the “Worker access rights” report see who can access data and if they can access information from anywhere in the world.</p>	Risk reduced to minimal where IP restrictions are implemented	
Data extracted from application kept insecurely	<p>mCare provides the capability to extract data using secure APIs. This is designed for use with 3rd party reporting solutions.</p> <p>Using the API is taking data out of mCare and no longer within any of PCS’ infrastructure or control.</p> <p>API keys are linked to user accounts in Monitor and will only allow access to data that the associated user has privileges to.</p>	<p>IP address restrictions also apply to APIs. Implementing this measure will ensure data is only accessed when people are located at authorised locations.</p> <p>Access logs include tracking where data has been accessed via the</p> <p>Ensure that 3rd party solutions remain in a secure compliant infrastructure and that access is controlled and encrypted appropriately.</p>	Risk is accepted by the care provider that further handling and processing of data extracted from mCare is done so appropriately.	

		<p>If data extracted and is subsequently transmitted further, consider if this is necessary and consider the method of transmission (e.g. using secure email services such as NHS mail). It may be necessary to lock down email and computer storage (such as USB ports) and implement measures so that all data is encrypted. Keep in mind that there are also websites that allow data to be uploaded, such as Dropbox and Google Drive. Data that is exported from mCare can be extremely expensive to fully secure, so best practice is to keep the people authorised for this to an absolute minimum.</p>		
<p>An enrolled device is left unattended or goes missing, and accessed by unauthorised user</p>	<p>The Care App is designed for contemporaneous evidence of care; this intrinsically means that staff using mobile devices will need to carry the device with them throughout their shift.</p>	<p>PCS supplied Android devices can use NFC lockdown tags, which provide additional security to ensure an NFC Tag must be used within the Location to unlock a device.</p> <p>N.B. to enable this feature, please contact clientsuccess@personcentredsoftware.com</p> <p>Other devices can use Secure PIN for users to access the physical device to reduce the risk of a device being accessed by unauthorised persons (such as a resident, relative or visitor etc.).</p> <p>Implement IP address restrictions so that if a device is taken outside of the permitted network; then data cannot be accessed.</p> <p>If a device cannot be found; ensure that it is disabled from the enrolled list of devices immediately upon notifying that the device cannot be located. Use the Status of Devices to view details of each device that has been used with the Care App and to disable access for any unauthorised devices.</p>	<p>Risk to be accepted by providers.</p> <p>Risk minimised where secure PINs are used</p> <p>Risk minimised when using PCS supplied Android devices and using the NFC lockdown feature</p>	

		<p>When devices are not in use or are charging, they should be kept in a secured location within the home to reduce risk of unauthorised persons picking up a device</p> <p>Providers should have an operational policy in regard to using the Care App and safe working practices.</p>		
An unauthorised device is used to access the Care App	<p>The Care App is freely available to download by anybody using the Google Play Store or App Store (Apple); however, a device must be enrolled to a location by authorised users</p>	<p>Ensure that Device enrolment and/or Admin rights are only given to authorised users.</p> <p>Providers should have an operational policy in regard to using the Care App and safe working practices.</p> <p>Use NFC location verification</p>	Risk minimised	
Inappropriate Sharing data with other software solutions through Integration.	<p>Significant benefit can be had by integrating data between applications (e.g. medication administration records integrated into mCare).</p> <p>Any information send from mCare to third party products is no longer protected by PCS</p> <p>The care provider is the data controller and the enabling and sharing of information through integrations is at the care providers discretion, and a risk assessment of the third party being integrated with should be undertaken.</p>	<p>Integration to other software applications can only be set up by users with system administrative rights and should only be done so with consultation with Person Centred Software.</p> <p>Once mCare has been integrated with other software solutions, should any concerns arise with the security of information shared with another software solution; then providers should advise PCS immediately and consider if the integration should continue or be disabled.</p>	Risk minimised	

<p>Users do not log-out of devices and another user picks up the device; leading to potential data breach or care being recorded under another user's name.</p>	<p>The nature of job, industry, working practice and mobile based solution means that devices will be passed from one user to another as shifts change over. Effectively devices may be in almost constant use. There is a risk that users do not log out before another person uses the device.</p>	<p>Users should be made aware that they are signing each care action and it is fraudulent to sign for another person's care actions.</p> <p>When devices are not in use or are charging, they should be kept in a secured location within the home to reduce risk of unauthorised persons picking up a device.</p> <p>All users at the same location will have the ability to view data on the Care App, so there is little risk in seeing information they are not entitled to see. If a user accidentally records information under another person's name; the care note correction process should be used to record this error.</p> <p>Users to be instructed to follow the finish work procedure / log-off when they have finished work and are placing the device back on charge or handing over to another person.</p> <p>Providers should have an operational policy in regard to using the Care App and safe working practices.</p>	<p>Care providers to accept risk</p>	
<p>User chooses to remember credentials on browsers</p>	<p>Web applications running on a browser typically prompt to store usernames and/or passwords.</p>	<p>Care providers to instruct users should be instructed to never store credentials on browser.</p> <p>Every computer should be set-up so that each person has a separate user account to access the computer, so that stored usernames/password are only stored for that user.</p> <p>Any device used to access mCare should only be used in a secure location</p>	<p>Care providers to accept risk</p>	

Device security compromised	Operating systems on devices are frequently being updated with security patches to prevent cyber attacks that may compromise data	Organisations should only use devices that are up to date with operating system security patches to ensure they are compliant with data protection recommendations. Mobile Device Management (MDM) should be deployed on devices and used to restrict access to approved apps and functions only; this reduces the risk of harmful software being used to compromise data.	Care providers to accept risk	
The email address used for login details is insecure meaning unauthorised persons compromising data	As some providers do not provide corporate emails to all staff; the email address entered is often made up or the email address used is a personal email address.	Where an email address is made up; the care provider must make sure that the user account is set up with a domain they are fully in control of or guaranteed to remain invalid.	Care provider to accept risk	The email address used for login details is insecure meaning unauthorised persons compromising data
Access given to relatives (or other contacts) where consent not in place	Relatives may be legitimately involved in a person's care or may have consent from a resident to access parts of their care plan through the Relatives Gateway	Prior to giving relatives (or any other person) access to the resident's information via the Relatives Gateway, providers must: <ul style="list-style-type: none"> - Verify the identity of the person they are giving access to • Verify they have appropriate consent and legitimate cause to access data Record in mCare that appropriate consents are in place	Care provider to accept risk	Access given to relatives (or other contacts) where consent not in place
Relatives gateway web components are imbedded into an insecure site.	The relatives gateway can optionally be embedded into providers own websites. If the site is insecure there is a risk of data being illegally accessed.		Care provider to accept risk	

Please add any other risks you identify as a result of reading this toolkit and seeking other advice necessary.



mCare Security Features

Security of Data is vital in the digital age; because of this we provide a series of security features to enables providers to stay in control and keep data secure.

Restricting access to Monitor by IP address	Optional	<p>To prevent access to Monitor from locations outside of the organisations network infrastructure; Organisation can set up IP address restrictions to control access to Monitor based on the IP address of where the request is made from.</p> <p>The IP restriction for accessing Monitor is set at an Organisation level. To set this up, providers will need to provide/set up a list of permitted IP address.</p> <p>Suitable network infrastructure will need to be supplied, and providers should seek advice from competent IT personnel, to ensure continuity of service and to assist with set up and maintenance.</p>	<p>Only Admin users can access/manage this feature</p> <p>Setting managed globally for the Organisation</p>




		<p>Individual user accounts can be set up as an exception to the IP restriction; meaning users will be able to access from any internet connection.</p> <p>Other considerations when implementing this feature: What about Remote workers (IP address, VPN)? Contingency plans (e.g. alternative networks, tethering, mobile data networks)?</p> <p>The IP address restriction also applies to any API calls made, for instance if using a reporting tool to extract JSON data using the secure API.</p>	
Restricting access to Care App by IP address	Optional	<p>Devices running the Care App are enrolled to a location. IP restrictions can be applied to a location, so that the Care App can only be used in the designated location.</p> <p>Consideration should be given as to whether users may need to use the device outside the network infrastructure (e.g. escorting residents to hospital, activities in a location other than the care home) before deciding to implement this feature.</p>	<p>Only Admin users can access/manage this feature</p> <p>Setting managed per location</p>
Requiring a location tag to enable login to Care App	Optional	<p>Using NFC tags programmed to the location ID; when this feature is enabled (only available to organisations with the Enterprise license).</p>	<p>Only Admin users can access/manage this feature</p> <p>Setting managed per location</p>
Password policy	Optional	<p>Organisations are able to set several password policy parameters within the Organisation Customisation settings; these settings cover the following:</p> <p>Password expiry days – Number of days from when the password was created that it will have to be reset</p> <p>Password minimum length – The minimum character length the password must be</p> <p>Password must have upper and lower characters – Indicates whether the password must contain upper and lower characters</p>	<p>Only Admin users can access/manage this feature</p> <p>Setting applies to Organisation</p>

		Password must contain symbols – Indicates whether the password must contain at least one symbol	
Device PIN to access	Optional (at device level)	<p>Whilst not part of the mCare product itself, it is recommended that devices are locked down with a PIN to control access to the device itself and a suitable timeout created.</p> <p>This can be set using Mobile Device Management (MDM).</p> <p>Devices are shared, meaning this PIN will need to be known by staff who use the Care App, but should not be shared with other staff or persons that do not need to have access.</p>	<p>Managed and controlled outside of mCare product.</p> <p>Can be set using MDM (Mobile Device Management) where applicable</p>
Forgotten Password	Standard* *Only if using a real email address	<p>The login for user accounts is in the format of an email address.</p> <p>To use the 'Forgotten password' feature, email addresses must be valid, so that users can reset their password via a link sent to their email address.</p> <p>As some providers do not provide corporate emails to all staff; the email address entered is often made up. Where an email address is made up; the care provider must make sure that the email used is guaranteed to be a domain they are fully in control of or guaranteed to remain invalid.</p>	Applies to individual logins.
User Access Rights	Standard	<p>mCare is a care delivery application; any worker with a user account created will be able to login to an enrolled device and view data for residents and/or enter care notes for residents at the communities/locations they have access to.</p> <p>Additional user access rights are given to each user account and should be based on what the individual workers job functions. Only staff who have the access right for 'Manage staff and run staff reports' will be able to amend other user's access rights.</p>	Access rights are granted in the worker record when editing the file.

Worker Access Report	Standard	A report that shows details of dates data has been accessed for the record you are viewing, the type of access and the type of data. This includes any data accessed via system APIs.	Report is accessed from worker records by clicking the  icon. Only users who are named as the Organisation Clinical Manager can view the report.
Worker Access Summary Report	Standard	The report shows details of dates data has been accessed, the type of access and the type of data. This includes any data accessed via system APIs.	Report can be run from the Process Data Security Worker access summary Only Admin users can access/manage this feature
Worker Access Log Report	Standard	The Home Manager or Responsible Person can view the 'Worker access log' to see which parts of mCare the person has accessed.	Report is accessed from worker records. Only users who are named as the Organisation Responsible person can view report.
Audit Records Report	Standard	Audit records can be viewed throughout mCare to allow for visibility of who has accessed various records across a defined period and what changes a user has made.	Report can be accessed via two methods: By default, the Audit records report can be accessed within certain records by clicking on the  icon. Report can also be run from Process Data Audit Records. Report can be run by users with the Change communities/sites and organisation customisation access rights
Service User Accessed Report	Standard	The named Home Manager or Responsible Person can view who has had access to Service User records. The report shows details of dates data has been accessed, the type of access and the type of data. This includes any data accessed via system APIs.	Report is accessed from worker records. Only users who are named as the Organisation Responsible person can view report.

Worker Access Rights report	Standard	<p>Users with system administrator level access rights can run a report to audit the 'Worker access rights'. The report displays individual user access rights for each Community that worker has access to, as well as their Role and Job Description to allow system administrators to check whether that worker has the correct access for their role.</p> <p>The report also highlights the password age, if password has never been changed and whether current set up means they can access from anywhere.</p>	<p>Report can be run from the Process Data Security Worker access rights</p> <p>Report can be run by users that have Manage staff and run staff reports access rights</p>
Status of Devices Report	Standard	<p>The 'Status of Devices' report enables administrators to view details about the devices that have accessed the application; details include</p> <ul style="list-style-type: none"> - IP address accessed from - Device ID - Location enrolled to - Last contact - Last known user - Last login/logout - Status/Active <p>This feature is only available to users with system admin rights only.</p>	<p>Report can be run from the Admin menu</p> <p>Only Admin users can access/manage this feature</p>
Disable a Device	Standard	<p>Using the 'Status of Devices' report; providers can drill down into the device details and disable access. Disabling access will effectively un-enrol a device and prevent users from logging in to the application.</p> <p>The feature is only available to users with system admin rights only.</p>	<p>Only Admin users can access/manage this feature</p>
Mobile Device Management (MDM)	Standard (when devices through PCS); Optional when providing own devices	<p>MDM is recommended to improve security by providing the ability to lock down devices to restrict access to only approved applications, standardise settings and manage profiles, updates and operating system versions.</p>	

Removing Users	Standard	When a member of staff leaves, the person who is responsible for managing their record will need to ensure their user account is removed. The user record is automatically removed when their associated staff file is closed, but the user record can be removed manually without closing the staff file where necessary (e.g. if temporary suspended from duties)	Users with the Manage staff and run staff reports permissions can create and remove user accounts from a staff file.
Device Enrolment	Standard	Devices must be enrolled to a location for users to access data using the Care App Users can only enrol a device to the locations they have access to.	Only users with Change communities/sites and organisation customisation i.e. System Admin or where they have specifically granted the Allowed to Enrol Devices for carers to use permission can enrol a device.
Community/Location Security	Standard	The community a person is in determines which other communities they have access to, and thus which records they'll have access to.	<p>For Staff Records: Community settings can be added/updated within the staff file – click Edit details for existing files.</p> <p>Users must have the Manage staff and run staff reports access rights</p> <p>For Service User Records: Community settings can be added/updated within the Service User file – click Edit details for existing files.</p> <p>Users must have the Change care delivery information and manage service users access rights.</p> <p>Configuring Communities/Locations: In order to configure and create new Communities/Locations, the User must be an Admin and have the Change communities/sites and organisation customisation access rights</p> <p>To add or edit a Community, got to the Admin menu click Organisation details select the Location/Community and click Add community.</p>

Care Note Correction Process and Voiding	Standard	Care notes cannot be deleted, they can only be voided or corrected. Where a care note has been corrected the original author will need to login and approve the changes	Care Notes can be checked by selecting a Service User File, then click Care Notes and select a care note. The Care Notes report allows a user to view care notes over a specific time period and any voided care notes.
User account locked	Standard	If a user attempts to login in unsuccessfully, after 30 attempts they will be locked out for 10 minutes.	
Enterprise help	Standard (with enterprise license)	mCare supports the ability for organisations to add their own help/guidance on each page of Monitor. Help content can be flagged to prompt all users or new users to read content when they open the relevant page.	Enterprise Help can be added by clicking on the help icon  and selecting Add enterprise help . Only Users with the Change communities/sites and organisation customisation access rights can add Enterprise Help.
Two Factor Authentication	Optional	Two-Factor Authentication (2FA) is a security method that requires two forms of identification to access data. An example of this is entering in a code from an authentication app.	For details on how to implement 2FA please see our user guide “User guide – 2FA” on the help page, which can be accessed via Monitor by clicking on the help icon  .
Single Sign On	Optional	Single Sign On (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites, using one set of company/corporate credential, centrally managed by your organisation.	For details on how to implement SSO please see our user guide “User guide – SSO” on the help page, which can be accessed via Monitor by clicking on the help icon  .

Example Operational Policy

Use of Care App by Care Staff

As all care providers are unique, Person Centred Software is not qualified to advise on the actual clinical use of mCare. This policy is intended as a guide to general system usage and purpose.

Operation of the Care App (devices):

- It is intended that each member of staff who are providing care are allocated a device for the entirety of their shift. When starting work; care staff should first log onto the device and read the shift hand over (h/o) notes, during shift h/o the shift leader should use monitor shift h/o report to ask if the carers have anything to add. At the end of their shift carers should return the devices to the shift h/o location, log off and put them on charge in the designated area accessible by all staff who require a device.
- It is the responsibility of the care staff who have logged into a device, to ensure that it is kept with them at all times throughout their shift.
- Users are responsible for maintaining the integrity of their password and to change it from the default password that has been allocated.
- Staff are expected to check the Service Users' record on the device prior to delivering care and to evidence care contemporaneously at the time of providing it whilst with the resident or as soon as possible after.
- If in the unlikely event carers cannot log off / finish work on the devices, they should do a verbal h/o with the lead (e.g. if internet failure prevents finish work / log off).
- The shift lead should use monitor shift handover reports to update handover notes prior to the start of the next shift.

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 mCare.

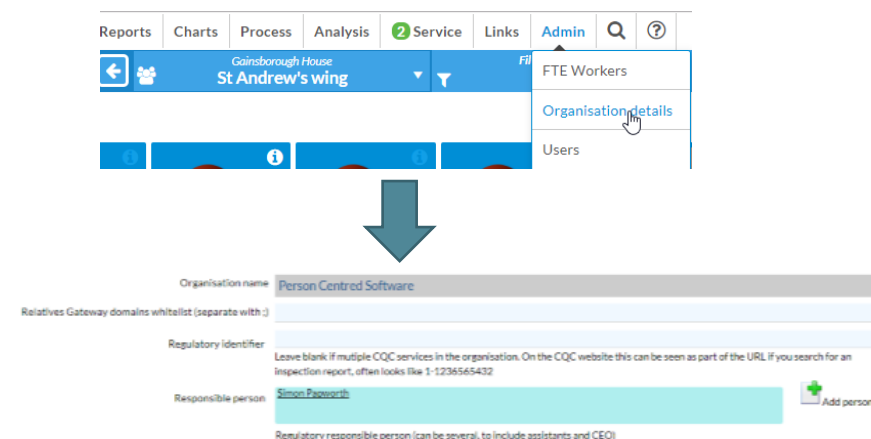
PCS will aim to notify customers within **24 hours** of becoming aware of the data breach.

Responsible Person

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

You will 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 GDPR, 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.

Addendum 1 - Person Centred Software and Brexit

As part of preparing for Brexit Person Centred Software have been keeping up to date on the latest guidance from the ICO (Information Commissioner's Office) and NHS Digital to ensure that our service provision remains unchanged after the Brexit Transition.

This is to inform you of the steps we have taken to ensure that nothing changes and that you can continue to use our service uninterrupted.

Terminology

- **EEA** – European Economic Area
- **ICO** – Information Commissioner's Office
- **Data Subject** – Staff and Residents
- **Data Controller** – Individual Care Homes / Organisations
- **Data Processor** – Person Centred Software
- **Sub Processor** – A party contracted by Person Centred Software to provide services.
- **SCC** – Standard Contractual Clauses

Brexit and Data Processing / Storage

From the 1st of January 2021 the UK left the EEA and became a 3rd Country under EU GDPR laws, the EU GDPR laws transitioned to UK GDPR laws with countries within the EEA transitioning to falling outside of the UK GDPR.

As of writing the UK has decided to grant an Adequacy decision with regards to the EEA and data transfer / storage what this means is that the UK recognises that the EEA has in place laws and standards to ensure data security to the same level as in the UK. This means that transferring data to the EEA or storing data in the EEA is permitted without additional safeguards or conditions required. As of 28th June 2021 the EU reciprocated with an approved adequacy decision for the UK.

To be clear the EU/UK GDPR laws do not prevent storage or processing of data in any country worldwide, they require that such processing / storage be performed in a secure way with the same protections as in the UK, this must be guaranteed through appropriate safeguards unless an Adequacy decision is in place.

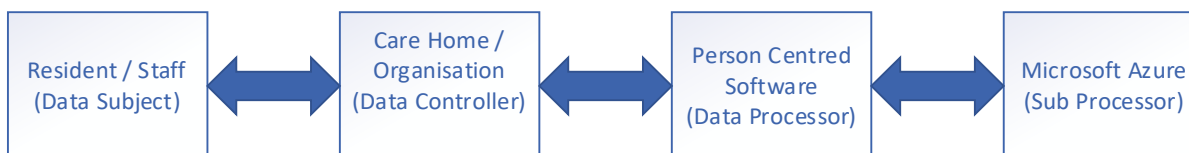
NHS Guidance currently states that the Storage and Processing of personal health related data in the EEA is allowed without additional safeguards.

Person Centred Software

Person Centred Software utilize Microsoft Azure for hosting services as a sub-processor, specifically we use a combination of the Azure West Europe region hosted within the EEA and the UK south region, as above the UK Adequacy decision ensures that the continued transfer of data to the EEA is allowed and considered safe.

Data Flow

The following shows the data flow between Data Subject to Controller and Processors



UK based Care Homes

For UK based care homes, the above referenced Adequacy decisions mean that nothing has changed in how the service Person Centred Software provides to you operates and your contract with us.

While SCCs are not required for the transfer of data to the EEA we will be happy to provide signed SCCs if requested.

EEA based Care Homes

For EEA based care homes while your data is stored in the EEA, as part of providing the service to you and supporting you Person Centred Software may access and process your information in the UK.

The UK has been granted adequacy by the EU this reciprocates the UK granting of adequacy to the EU, as such personal data as described in EU GDPR and UK DPA is legally allowed to transfer in both directions between the UK and EEA.

Person Centred Software already hold SCCs between us and Microsoft Azure as such we will be updating our Terms and Conditions to include the EU SSCs this will bind us to the same standards as you with regards to data protection and is accepted by the EU as an appropriate safeguard.

The chain of SCCs allows for the transfer of data to any country / company that is not covered by an adequacy decision.



Conclusion

Hopefully this reassures you that your continued use of Person Centred Software will remain legal under both EU and UK GDPR laws and that all required steps have been taken to ensure that data can continue to flow uninterrupted after the Brexit transition.

If you have additional questions about this or concerns please contact our Client Success team at: clientsuccess@personcentredsoftware.com