Document Title:	**Care Monitor Limited Data Protection Policy CMPPP**
Version.	**1**
Prepared by:	**Eithne Ni Dhomhnaill, Tom Duffy and Brian O' Neill, Care Monitor Ltd.**
Issue date:	**July 2018**
Review date	**July 2021**
Authorised by:	**Eithne Ni Dhomhnaill, Managing Director.**

1.0 Policy Statement.

It is the policy of Care Monitor Ltd. that at all times activities relating to the operation of its business will comply with data protection legislation.

2.0 Purpose.

The purpose of this policy is to outline the arrangements and processes in place to ensure that Care Monitor Ltd complies with its obligations under data protection legislation.

3.0 Objectives.

3.1.1 To ensure that Care Monitor Ltd is compliant with data protection legislation in all activities related to the operation of the business.

3.1.2 To ensure that employees and third party contractors understand their responsibilities when carrying on any activities related to the business of Care Monitor Ltd.

3.1.3 To ensure that customers are informed of the arrangements in place for Care Monitor Ltd to comply with its obligations under data protection legislation and any responsibilities of customers when accessing services from Care Monitor Ltd.

4.0 Scope.

This policy applies to the following:

1. All employees and third party contractors providing a service to Care Monitor Ltd.

2. Customers using the services of Care Monitor Ltd.

The policy applies to all processing of personal data and special categories of personal data carried out by Care Monitor Ltd.

5.0 Definitions.

5.1 **Data Subject.**

A data subject refers to an identified or identified living person (GDPR). It is the individual the personal data relates to (Data Protection Commissioner, 2017). In the context of this policy a data subject is any living person whose personal data is obtained and processed by the centre. For example residents, employees, residents' representatives or family members whose personal data is obtained and processed by the centre.

5.2 **Personal Data.**

Personal data means any identifiable information relating to a living individual ('data subject'). This means information by which the individual can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person (General Data Protection Regulation).

5.3 **Special categories of personal data.**

Refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5.4 **Genetic Data.**

'Genetic data' means *'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;'* (General data Protection Regulation).

5.5 **Biometric data.**

Biometric data' means '*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprints) data';* (General data Protection Regulation).

5.6 **Data Concerning Health.**

'Data concerning health' means *'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;'* (General data Protection Regulation).

5.7 **Data Controllers.**

A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files. Data controllers can be either individuals or "legal persons" such as companies, Government Departments and voluntary organisations. Examples of cases where the data controller is an individual include general

practitioners, pharmacists, politicians and sole traders, where these individuals keep personal information about their patients, clients, constituents etc https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm. accessed 11/04/2018.

5.9 Processing

'processing' means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' (General Data Protection Regulation).

5.10 Disclosure

Disclosure refers to the release of personal data or personal information to a third party outside of the original specified purpose of obtaining the data / information. (Data Protection Commissioner, 2013)

5.11 Privacy

In terms of personal health information, privacy can be described as the right of individuals to keep their information confidential and is a human right enshrined in both Irish and European legislation. (HIQA, 2017).

5.12 Third Party

'Third party' means 'a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data; (General Data Protection Regulation).

5.13 Consent.

'Consent' of the data subject means 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (General Data Protection Regulation).

5.14 Personal Data Breach.

Personal data breach' means 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;' (General Data Protection Regulation).

6.0 Responsibilities.

6.1 **Care Monitor Personnel.**

6.1.1 Care Monitor Personnel have a responsibility to ensure that the processing of personal data and special categories of personal data is carried out in accordance with the legal and professional framework outlined in this policy.

6.1.2 Care Monitor Personnel are not permitted to process any personal data unless the data subject has given permission or there is another legal basis for such processing such as to comply with one or more of the statutory obligations outlined in 7.1 of this policy.

6.1.3 Care Monitor personnel must safeguard the confidentiality of all personal data accessed in the course of their work and must not disclose any personal data without the expressed permission of the data controller.

6.1.4 Where, in the course of providing support services or training to a customer, a member of Care Monitor personnel is privy to personal data including special categories of personnel data, the member of Care Monitor personnel is not permitted to process or disclose this information to third parties.

6.1.5 Where in the course of their work, a member of Care Monitor personal suspects that a personal data breach has occurred or becomes aware that a data breach has occurred, he/she must comply with the protocol for responding to a suspected or actual data breach outlined in this policy.

6.2 **Third Parties Acting on behalf of Care Monitor.**

6.2.1 Employees and personnel of Nursing Matters & Associates who carry out activities on behalf of Care Monitor Ltd must also comply with the requirements set out in 6.1 above.

6.2.2 Other third parties, specifically Datastring and BigMind by Zoolz.have specific responsibilities to ensure that they process personal data and special categories of personnel data in accordance with legal requirements.

6.2.2 Third parties must inform Brian O' Neill without undue delay of any suspected or actual data breach related to personal data being processed on behalf of Care Monitor.

6.3 **Customers.**

6.3.1 In accordance with the contract between Care Monitor Ltd and a Customer, the Customer is the data controller and must ensure that he/she is entitled to transfer any personal data, including special categories of personnel data to Care Monitor for backup where there is service is part of the contract.

6.3.2 Where personal data is being processed based on informed consent, the Customer must ensure that data subjects, whose personal data is transferred for backup have been informed of and have given their consent to same.

7.0 Legal and Professional Framework for Records Management.

7.1 **Legal Basis for Processing Personal Data.**

7.1.1 Under European and national data protection legislation, processing of personal data is lawful only *(referred to as the 'legal basis' for processing personal data)* if and to the extent **that at least one** of the following applies:

a) The data subject has given consent to processing his/her personal data for one or more specific purposes. This consent is subject to conditions outlined under

b) The processing of the data is necessary for performance of a contract to which the person is party or to take steps at the request of the person prior to entering into a contract.

c) Processing is necessary for the controller to comply with a legal obligation.

d) Processing is necessary to protect the vital interests of the person or of another living person.

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller.

f) Processing is necessary for the purposes of the legitimate interests pursued by the controller

or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7.1.2 In addition to the conditions outlined above, the processing of personal data is only lawful if it complies with the principles outlined in 6.5

(Data Protection Act, 1988 and 2003; Data Protection Bill, 2018).

7.2 **Processing of special categories of personal data.**

Special categories of personal data refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Processing of special categories of personal data is allowed only if it complies with the principles outlined in 6.4 **and one** of the following applies:

a) The data subject has given explicit consent to the processing of the special category of personal data for one or more specified purposes (Data protection Bill, 2018).

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social welfare law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (Data Protection Bill, 2018; General Data Protection Regulation).

c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (General Data Protection Regulation) including to prevent injury or other damage to the data subject or another individual and to prevent loss, in respect of, or damage to property (Data Protection Bill, 2018).

d) Processing relates to personal data which are manifestly made public by the data subject; (General Data Protection Regulation).

e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (General Data Protection regulation) including for the purpose of obtaining legal advice or in connection with legal claims,

prospective legal claims, legal proceedings or prospective legal proceedings (Protection Bill, 2018).

f) Processing is necessary for medical purposes and is carried out by or under the responsibility of a health practitioner or a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that duty of confidentiality owed by a health practitioner.

g) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions of professional secrecy (General Data Protection Regulation).

h) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

i) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

8.0 Principles relating to processing of personal data.

Under European and national legislation, the centre is obliged to ensure that personal data is

1. Obtained and processed fairly, lawfully and in a transparent manner in relation to the data subject.

2. Information is collected only for one or more specified, explicit and lawful purposes

3. Information is used and disclosed only in ways compatible with these purposes

4. Information is kept safe and secure

5. Information is kept accurate, complete and up-to-date

6. Information is adequate, relevant and not excessive

7. Information is retained for no longer than is necessary for the purpose or purposes and according to legal requirements.

8. Data subjects e.g. Residents can have a copy of his/her personal data to an individual, on request, except in specific circumstances outlined in the legislation below.

9.0 Professional Requirements.

Nursing Matters & Associates who provide training services to clients on behalf of Care Monitor Ltd are also obliged to comply with professional codes, standards and guidance related to residents' personal information. These include:

- Nursing and Midwifery Board of Ireland 2015 Recording Clinical Practice, guidance to Nurses & Midwives.
- Nursing and Midwifery Board of Ireland 2014 Code of Professional Conduct and Ethics for Nurses & Midwives.

10.0 Protocol for Obtaining and processing Personal Data by Care Monitor Ltd.

10.3 **Legal Basis for processing Customer data.**

10.3.1 Care Monitor Ltd obtains and processes Customer data for the following lawful reasons:

1. The processing of the data is necessary to take steps at the request of the customer prior to entering into a contract, such as to send information about the software to the prospective customer and or to arrange a demonstration.

2. The processing of the data is necessary for performance of the written contract to which the customer is party. Subject to the terms of this written contract, Care Monitor Ltd acts as a processor on behalf of and with the authorization of the customer, who is the controller for the data being processed.

3. To comply with legal obligations under the Companies Act, 1990 and the Value Added Tax Consolidation Act, 2010.

4. Processing is carried out with the consent of the customer in order to send information about products and services of Care Monitor Ltd.

10.4 **Categories of Data Subjects.**

Care Monitor Ltd obtains and processes information on both potential and actual customers for the purposes of entering into an agreement about the provision of services. As part of the provision of services to clients, subject to a signed contract between both parties, Care Monitor Ltd may also store personal data on the following data subjects:

1. Customers.
2. Staff who are designated by the client to act as a focal contact person between the client and Care Monitor Ltd.
3. Employees of the Customer whose personal data has been entered into the relevant module of Care Monitor.
4. Residents in the healthcare facilities owned and operated by customers.

10.5 **Categories of Data Processed.**

Care Monitor may process the following categories of data on behalf of Customers subject to the terms of the signed written contract:

1. Personal data for clients, designated staff and residents.
2. Special categories of personal data, which subject to the terms of the written agreement may be stored by Care Monitor Ltd on behalf of and under authorisation of the customer.

11.0 Adherence to Principles of Data Processing.

11.1 **Obtained and processed fairly, lawfully and in a transparent manner in relation to the data subject.**

Following an initial enquiry from an individual about products and services and where the individual requests same, an email is sent to the individual with the required information. This email contains a link to Care Monitor Ltd.'s Privacy Policy.

11.2 **Information is collected only for one or more specified, explicit and lawful purposes.**

Personal data and special categories of personal data are collected only for those lawful purposes outlined in 6.3.1.

11.3 **Use and disclosure of personal data in ways compatible with these purposes.**

Care Monitor is obliged both under data protection legislation and the terms of the written contract between itself and the Customer to use and disclose personal data only in ways compatible with the purpose for which it was obtained. Customer data will be used only as required for the purposes of the performance of the contract agreed between the Customer and Care Monitor Ltd and subject to the terms of the contract. Additional processing for direct marketing purposes will only occur where the Customer has given explicit consent for such processing. This is facilitated through an email that is sent to each customer after the initial contact, which specifically asks for the customer's consent to contact them in the event of new products and / or services being developed.

We do not share customer details with any other third parties for the purposes direct marketing by those parties.

11.3.1 Processing of Customer data.

Personal data pertaining to Customers is stored in manual and electronic format and processed and accessed only by staff of Care Monitor Ltd or third parties acting on behalf of Care Monitor Ltd. Personal data of Customers may be shared with Ecovis accountancy services in order to assist Care Monitor Ltd meet its statutory obligation under the Companies Act, 1990 and the Value Added Tax Consolidation Act, 2010. Personal data and special categories of personal data obtained by the Customer from third parties, such as staff or residents may be stored for back up purposes by Datastring Ltd on behalf of Care Monitor Ltd, subject to the terms of agreement of the written contract between the Customer and Care Monitor Ltd. Staff of Care Monitor Ltd or third parties acting on behalf of Care Monitor Ltd are not authorised to process Customer data other than for the explicit purposes for which the data was obtained and the uses outlined in the written contract.

11.3.2 Processing of Customer data relating to third parties.

Where Care Monitor Ltd acts as a data processor for a Customer, it may lawfully process the personal data of third parties when authorised to do so by the Customer who is the data controller for such data. Where Care Monitor Ltd is requested to store third party personal data, under the terms of the written contract, the customer is required to ensure that it is lawfully entitled to authorise Care Monitor Ltd to store the relevant personal data on its behalf.

3. Information is kept safe and secure.

Personal data related to customers of Care Monitor ™ is stored on encrypted laptops and desktops of the staff of Care Monitor. Backups are stored securely and encrypted in a cloud backup maintained by Datastring LTD. and BigMind by Zoolz.

Data relating to Staff and Residents, which may be stored on Care Monitor, is not stored by Care Monitor LTD, but rather by the customers. Some customers have access to our Cloud Backup service hosted by Datastring LTD which is encrypted before backup to their cloud.

We may have access to data while installing, supporting or training our customers and their staff, however all Care Monitor staff and third parties acting on behalf of Care Monitor LTD are not permitted to store or disclose any of this information, unless specifically requested to do so by the customer's data controller, and only with those persons specifically designated by the customer's data controller.

4. Information is kept accurate, complete and up-to-date.

   Customer data is obtained and processed as required where the data is necessary for performance of a contract to which the Customer is party or to take steps at the request of the Customer prior to entering into a contract. This information is provided by the Customer and only amended where the Customer informs Care Monitor Ltd of a change in information.

   Personal data including special categories of personal data relating to residents and / or staff is stored as part of an agreed backup service contract with the Customer as outlined in 3. It is the responsibility of the Customer as data controller to ensure that this information is kept accurate, complete and up-to-date.

5. Information is adequate, relevant and not excessive.

Information obtained from Customers is limited only to that information that is necessary for the performance of a contract agreed with the Customer, such as name, contact details and information for accounts.

Personal data including special categories of personal data relating to residents and / or staff is stored as part of an agreed backup service contract with the Customer as outlined in 3. It is the responsibility of the Customer as data controller to ensure that this information is adequate, relevant and not excessive.

6. Information is retained for no longer than is necessary for the purpose or purposes and according to legal requirements.

Customer information obtained for the purposes of performance of a contract, including financial aspects of the contract are retained for a period of 6 years from the data of the last transaction or termination of a contract. There may be occasions where to comply with a legal obligation Care Monitor may need to retain information for a period of more than six years. Where these circumstances arise, the Customer will be informed beforehand.

Personal data including special categories of personal data relating to residents and / or staff is stored as part of an agreed backup service contract with the Customer as outlined in 3. It is the responsibility of the Customer as data controller to ensure that this information is retained for no longer than is necessary for the purpose or purposes and according to legal requirements. Care Monitor will delete information only where requested to do so by the Customer as data controller of this information.

7. Data subjects can have a copy of his/her personal data to an individual, on request, except in specific circumstances outlined in the legislation below.

Care Monitor will make available to a Customer a copy of his/her personal data processed by the company on request in accordance with legislation.

It is the responsibility of the Customer as data controller to make arrangements to meet the rights of data subjects with regard to access to their personal data including special categories of personal data. Care Monitor on request of the Data Controller will provide information on how to provide a copy of the data subjects personal information, including special categories of personal information stored using Care Monitor software.

In the event of a termination of the contract between Care Monitor and the Customer, Care Monitor will do the following;

1. Terminate any backups and provide the latest backup to the customer.

2. Provide a read-only version of Care Monitor, so that existing data may still be viewed or printed by the customer or deleted according to their own data protection policies. Care Monitor will not retain any of the customers data stored using Care Monitor relating to the customer's data subjects, and terminate its responsibility as data processor.

13.0 Protocol for Responding to a suspected or actual personal data breach.

13.1.1 A personal data breach is a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (GDPR)

13.1.2 "Destruction" of personal data is where the data no longer exists, or no longer exists in a form that is of any use to the controller (Article 29 Data Protection Working Party, 2018)

13.1.3 "Damage" is where personal data has been altered, corrupted, or is no longer complete (Article 29 Data Protection Working Party, 2018)

13.1.4 "Loss" of personal data, is interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession (Article 29 Data Protection Working Party, 2018)

13.1.5 Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR (Article 29 Data Protection Working Party, 2018)

13.1.6 Breaches can be categorised as:

1. "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.

2. "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

3. "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

13.1.7 Depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

13.1.8 A security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. A breach involving the temporary loss of availability should be documented in accordance with Article 33(5).

13.1.9 ***Where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12)***

(Article 29 Data Protection Working Party, 2018)

13.1.10 Under Article 33 of the GDPR, when the centre becomes aware of a personal data breach, it must report the breach to the Data Protection Commission without undue delay and not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the centre does not notify the Data protection Commission within 72 hours, the late notification must be accompanied by a written explanation of the delay.

13.2 **Procedure for Responding to an actual or suspected breach of personal data.**

13.2.1 All Care Monitor Personnel or Nursing Matters & Associates personnel acting on behalf of Care Monitor, must report any suspected or actual personal data breaches to Ms. Eithne Ni Dhomhnaill or his/her deputy immediately.

13.2.2 Third parties providing backup must report suspected or actual data breaches to Mr. Brian O' Neill.

13.2.3 When either Mr. O Neill or Ms. Ni Dhomhnaill are informed of a suspected or actual data breach, both will carry out an initial internal investigation to establish whether or not a data breach has occurred.

13.2.4 If the investigation determines that in fact a personal data breach has occurred involving residents or staff of a Customer, the Customer will be informed immediately.

13.2.5 If the investigation determines that in fact a personal data breach has occurred and is assessed as resulting in risks to the data subjects, Ms. Ni Dhomhnaill will complete a first notification to the Data Protection Commissioner no later than 24 hours after detection of the breach. If all the necessary information is not available at the time of the first notification, a second notification must be made within 3 days of the first notification.

13.2.6 Where it is determined that the data breach has occurred it is likely to result in a risk to the rights and freedoms of data subjects, Ms. Ni Dhomhnaill and Mr. O' Neill will identify and implement action(s) needed to address the breach.

14.0 References.

1. Article 29 Working Group, (2017) , Guidelines on Data Protection Officers ('DPOs') accessed 13/04/2018 at http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
2. Article 29 Working Group, (2018) Guidelines on Personal data breach notification under Regulation 2016/679 accessed 01/05/2018 at https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf
3. European Parliament and the Council of the European Union, 2016 General data Protection Regulation.
4. Government of Ireland, Data Protection Bill 2018.
5. Health Services Executive, DATA PROTECTION AND FREEDOM OF INFORMATION LEGISLATION Guidance for Health Service Staff accessed 01/05/2018 https://www.hse.ie/eng/services/list/3/acutehospitals/hospitals/ulh/staff/resources/pppgs/dp/dp.html
6. Health Services Executive, Data Breach Management Policy accessed 01/05/2018 https://www.hse.ie/eng/services/list/3/acutehospitals/hospitals/ulh/staff/resources/pppgs/dp/dp.html
7. Nursing and Midwifery Board of Ireland, 2015 Recording Clinical Practice, guidance to Nurses and Midwifes
8. Nursing and Midwifery Board of Ireland, 2014 Code of Professional Conduct and Ethics for Nurses and Midwifes
9. Data Protection Commissioner, (2017) Preparing Your Organisation for the General Data Protection Regulation.
10. Data Protection Commissioner, (2018) Rights of Individuals under the General data protection Regulation.
11. Irish College of General Practitioners, Data Protection Working Group (2018) Processing of Patient Personal Data: A Guideline for General Practitioners
12. Health Act 2007 (Care And Welfare Of Residents In Designated Centres For Older People) Regulations 2013
13. Health Services Executive (2012) Standards and Recommended Practices for Healthcare Records Management.