NCHA Position Statement

Impact of the General Data Protection Regulation in Clinical and Medicines Homecare Services

Scope
This report was commissioned by the NCHA Board to ensure a common understanding of the impact of the General Data Protection Regulation (GDPR) that came into force in EU Member States including the UK on 25th May 2018. Whilst there is some flexibility allowed in the national implementation, NCHA currently believes that the broad understanding outlined here is unlikely to significantly change, even post-Brexit. The Data Protection Act 2018, which supplements the GDPR, received the Royal Assent and its main provisions commenced on 25th May 2018.

This position statement considers the impact of GDPR on patient data only; for the purposes of this paper, patient data includes personal information about the patient’s friends, family and carers and the term patient data also includes the personal information of the patient’s carer(s). It is noted that GDPR also applies to the personal data of homecare provider’s employees, but for the purposes of this report this is out of scope, except where employees are identified within the patient records.

This paper has been developed as a discussion paper with a view to establishing a consensus view between NCHA, NHS and regulators to ensure a consistent understanding of the lawful bases of data processing in clinical and medicines homecare services.

For further information please contact info@clinicalhomecare.co.uk

NCHA Limited Registered Office: Ground Floor, 4 Victoria Square, St Albans, Hertfordshire, AL1 3TF.
A Private Limited Company registered in England and Wales No: 6642621

Disclaimer
NCHA does not warrant or represent that the material in this document is accurate, complete or current. Nothing contained in this document should be construed as medical, commercial, legal or other professional advice. Detailed professional advice should be obtained before taking or refraining from any action based on any of the information contained in this document.
Executive Summary

Compliance with RPS Professional Standards for Homecare Services and the requirements of the NHS Data Security and Protection Toolkit means most clinical and medicines homecare organisations already have robust information governance processes in place. Existing processes ensure patient identifiable data is held securely and patients are told how their personal data will be used. As such, the General Data Protection Regulation (GDPR) does not require wholesale changes to the way patient data is handled in clinical and medicines homecare services.

The presence of a lawful basis for processing patient data in clinical and medicines homecare services has not been challenged, however, there have been repeated discussions about the definitions of data processors and data controllers and which lawful basis applies. There is particular sensitivity for NHS clinical referring centres who do not want the patient data they provide to homecare providers to be further processed or used to offer other products and services direct to NHS patients outside the clinical and medicines homecare service without their knowledge or permission.

Both NHS clinical referring centres and homecare providers are independent data controllers. NHS clinical referring centres routinely using ‘performance of a task carried out in the public interest (public task)’ as the lawful basis of processing patient data and homecare providers routinely using legitimate interest as the lawful basis of processing patient data in the provision of clinical and medicines homecare services for NHS patients. This gives the homecare provider the flexibility needed to deliver all aspects of the clinical and medicines homecare service efficiently, whilst giving assurance to the clinical referring centre that their NHS patient identifiable data is not used in unexpected ways.

The Information Commissioner’s Office (ICO) recommends that “if consent is difficult, [organisations should] look for a different lawful basis”1. GDPR consent should not be relied upon because for health and care providers there are other more legally secure provisions within GDPR that would be more appropriate. Common law confidentiality requirements and the requirement for the patient to be informed about their treatment and to give their permission for treatment to continue are unaffected. Homecare providers have existing, robust practices that meet these common law requirements and these should continue in future. NCHA recommends using different terminology to ensure patients understand the difference between common law consent to treatment and GDPR consent to processing of their personal data; i.e. using the terminology “permission” for the former and using the unqualified term “consent” only to mean GDPR consent.

NHS clinical referring centres can be assured that patient identifiable data can only be processed for the legitimate interest of delivering the clinical and medicines homecare service which the NHS has commissioned. Whilst legitimate interest is a wide category, the homecare provider can only use the personal data in ways that patients would reasonably expect and this test must be strictly applied where special category data (e.g. health data) is being processed. In practice this means the patient’s personal data will only be used to provide the clinical and medicines homecare service as stated in the clinical referring centres clinical and medicines homecare service information and the homecare provider’s welcome pack. The information provided to patients by clinical referring centres and homecare providers varies between clinical and medicines homecare organisations; however, national standards and guidelines are in place. Clinical referring centres can be further reassured by reviewing the homecare provider’s “legitimate interests assessment” related to their particular clinical and

---

medicines homecare service. Furthermore, the patient data may not be used for electronic or telephone marketing, as legitimate interest lawful basis does not extend to any use which would otherwise require consent under the Privacy and Electronic Communications Regulations.

Whilst there has been much debate in the past, homecare providers consider themselves to be data controllers for the patient records that they generate. In order to be efficient and effective, homecare providers must control “how” the data is processed within the context of similar services being provided to many different NHS clinical referring centres. Homecare providers have their own regulated status and have requirements to keep information about the services they deliver. ICO guidance states that activities such as interpretation, the exercise of professional judgement or significant decision-making in relation to personal data must be carried out by a data controller.\(^2\) It is important to remember that there can be multiple data controllers of the same personal information.

Information about the homecare provider’s staff who deliver the service to individual patients is inextricably linked to the patient record. Whilst this means the homecare provider can determine “why” the patient identifiable data is used, these uses are severely constrained by the legitimate interest tests as described above which are documented in the “legitimate interests assessment”.

1. **Recommendations for Homecare Providers**

**Requiring immediate action**

1.1 Appoint a Data Protection Officer (DPO).
1.2 Assess which lawful bases apply to your organisation’s activities and document that assessment.
1.3 Update your Data Protection Policy and/or Privacy Notice. GDPR requires that your privacy notice should include your lawful basis for general processing as well as the purposes of the processing and any additional condition for processing “special category” data.
   - archiving purposes in the public interest;
   - scientific research purposes; and
   - statistical purposes.
1.4 Update Subject Data Access processes in line with GDPR (i.e. no fees to be charged, 30 day time limit for supply of subject data, 30 day requirement to correct inaccurate data).

**Must do in the first 12 Months**

1.5 Review and revise patient information leaflets to ensure transparency and that the legal basis of personal data processing is clear and includes the organisation’s commitment to “fair processing”. The ICO have published a code of practice on what should be included. The GDPR / Data Protection Act now requires specific information be provided to a data subject. Articles 12 – 14 of the GDPR set out what will be required. Each data controller must issue their own privacy notice to the patient when they first request or first receive patient identifiable data. Further information is available from the ICO.\(^3\)

---


1.6 Self-audit information governance processes relating to all patient data to ensure they are robust and enforced and appropriate records are always kept and document corrective and preventative actions arising. Develop and implement an action plan to resolve any issues identified.
  - Ensure all information assets containing patient data are robustly controlled
  - Review record keeping and archiving processes to ensure patient identifiable data is not kept for longer than is necessary
  - Ensure all flows of patient data are documented clearly, differentiating between data sharing between parties integral and essential to the clinical and medicines homecare service and any other data sharing
  - Where patient data is stored, processed or shared, ensure there is no other reasonable way to achieve that purpose
  - Any other data sharing must be in accordance with data sharing agreements and with explicit patient consent recorded before data is shared. The only exception should be where another lawful basis for the data sharing applies and is fully documented.
  - Ensure there is a process for archiving identifiable patient data to a restricted form in case a patient objects to further processing of their identifiable data.
  - Identify if, and where GDPR consent is used as the legal basis of data processing, check if existing DPA consents meet the standards required under GDPR and update consent if needed.

Ensuring longer term compliance
1.7 Review change control processes to ensure Data Protection Risk & Impact Assessments are performed or updated wherever patient identifiable data is involved in the change and ensure this is completed before implementation of the change.

1.8 Review contracts with sub-contractors to ensure they contain appropriately robust data protection obligations which are appropriate to the controller/processing relationships in question. Ensure that contracts reflect the obligations in relation to any sub-contracting which is contained in contracts with relevant purchasing authorities. The contract should reflect the obligations to the extent that those obligations are relevant (and in this context we note that in some circumstances the homecare provider is likely to be a controller in its own right and not simply a processor). GDPR requires that the contracts contain certain specified information.4

1.9 Review any instances of pseudonymised patient data sharing and revise processes accordingly to ensure anonymisation of the data. If the data cannot be anonymised treat as patient identifiable data.

1.10 Update risk assessments relating to all aspects of patient data renaming them as “Data Protection Risk & Impact Assessments” – they must be approved by the organisation’s Senior Information Risk Officer (SIRO) and Data Protection Officer (DPO).

1.11 Update training needs analysis relating to GDPR implementation should be performed and identified training needs should be met and training recorded.

---

2. Background

The GDPR has been implemented directly across all EU member states. It contains most of the legal obligations which are applicable to data protection. The GDPR gives member states some ability to make specific provision as to how GDPR applies in each state and the Data Protection Act (DPA) 2018 does this for the UK meaning that GDPR will still apply in the UK irrespective of the outcome of Brexit. It also deals with some matters which are not dealt with in EU law (i.e. the derogations) e.g. national security and immigration. It also repeals the Data Protection Act 1998. Within this document, the term "Articles" refer to GDPR Articles and “Sections” refer to DPA 2018 Sections.

Respect for patient confidentiality and the secure handling of patient identifiable data has been a feature of clinical and medicines homecare services since their inception. NCHA Members maintain compliance with the Information Governance Toolkit level 2 or above and are registered as organisations that hold personal sensitive data with the ICO and have appointed Caldicott Guardians to protect the interest of patients.

Compliance with RPS Professional Standards for Homecare Services and the requirements of the Information Governance Toolkit means most homecare organisations already have robust processes in place to ensure patients give informed consent to receive the clinical and medicines homecare service, patient identifiable data is held securely, data processing is fair and lawful, and patients are told how their personal data will be used. As such, the GDPR does not require wholesale changes to the way patient data is handled in clinical and medicines homecare services. However, the principles of “accountability” and “transparency” are added and there are some clarifications and definitions which homecare organisations must understand and homecare providers must update their Privacy Notices to ensure they remain compliant with the regulations. GDPR does not apply to anonymised patient data or data made public by the individual him/herself.

There has not been a challenge relating to the absence of a lawful basis for processing patient data in clinical and medicines homecare services; however, there have been repeated discussions about the definitions of data processors and data controllers and which lawful basis applies.

GDPR requires the lawful basis being used to be agreed prior to data sharing, to be documented and to be transparent to patients. It is therefore critical to reach consensus and document the lawful basis of data sharing in clinical and medicines homecare services at the earliest opportunity. Clear signposting to the Data Protection statements (i.e. the Privacy Notices) for each data controller must be in place for all data subjects, including identification of any organisation acting as data processor under the responsibility of that data controller. Data protection statements and clinical and medicines homecare service information for patients and carers will need to be reviewed to provide full disclosure of what personal data is used, for what purpose, who it is shared with, the legal basis for doing so and how long it will be retained.

Fines under the GDPR can be applied for any breach of the regulation, including process failures, not just where personal data has been compromised as previously. Fines are also significantly higher than before - up to a maximum of €20 million or 4% of global group turnover. As the clinical and medicines homecare industry accounts for £2.2 billion turnover,

---

fines have the potential to significantly impact clinical and medicines homecare industry notwithstanding that some clinical and medicines homecare providers are part of larger group organisations. Pharma manufacturers who fund clinical and medicines homecare services and pharma manufacturers who fund Patient Support Programmes will also need to be fully GDPR compliant if they receive, hold or process patient identifiable data. The General Data Protection Regulation 2016/679 and the Data Protection Act 2018 replaces the Data Protection Act 1998.

Health data is one of the “special categories” of data defined by the GDPR. “Special category” data is broadly similar to “sensitive personal data” under the Data Protection Act 1998. As health data is “special” there are no exemptions for small organisations. There are additional restrictions to the processing of “special category” data; however, these are unlikely to restrict clinical and medicines homecare activities as there are catch-all clauses that cover provision of healthcare to an individual, wider patient safety activities and archiving for scientific or historical research.6

3. Impact of General Data Protection Regulations in Clinical and Medicines Homecare Services

The actions needed by homecare providers are, in the main part, to tighten up documentation of processes that are already in place and to ensure any historical anomalies are resolved. GDPR introduces a new principle of “data protection by design and by default” meaning new services and changes must have privacy processes “built in” by undertaking a Data Protection Impact Assessment (DPIA).

The biggest impacts are likely to be in manufacturer funded services where there must be clearly defined “lines” between data held and used for the “standard” NHS medicines homecare service and the optional pharma funded Patient Support Programmes as the resulting data processing is likely to have a different legal basis.

4. Data subjects’ rights under GDPR

Patients can request access to the data held about them to be provided free of charge and this must be provided without delay and in any case within one month of the receipt of the request – only in exceptional circumstances, this can be increased to 2 months and charges may only be applied for repeated requests. Patients can request copies of their data in “portable” format only where consent is the legal basis for data processing and this right only applies to data that the patient has provided to the data controller to which the request is made.

Where GDPR consent is used as the lawful basis for data processing, a patient has a new right “to be forgotten”; however, there are a number of reasons why it may be inappropriate for organisations providing health and care services.

Homecare organisations may have reasonable grounds to refuse requests for the erasure of information for the following reasons;

- for public health purposes in the public interest;

- archiving purposes in the public interest, scientific research, historical research or statistical purposes;
- to help justify health and care decisions that may have been taken as a consequence of a clinician having seen the information in question; or
- the exercise or defence of legal claims.

Where the personal data must be retained and/or processed, the patient has a right to have the data updated or corrected if it is inaccurate or incomplete. Patients can request rectification of inaccurate data and this must be actioned within 1 month, this may be extended by a further 2 months in exceptional circumstances for complex requests. If the data controller decides not to make the amendments requested, the patient must be informed why and given information about how to complain or take further action.

Patients can ask for the processing of their personal data to be restricted. Irrespective of the legal basis for data processing, the patient’s objections to data retention or processing should be acted on where possible and if not, the objection and the legal reasons why it was not acted upon should be recorded and the patient informed.

Patients must be informed about and have a right to object to any decision made solely via computer algorithm without the intervention of a clinician. This may apply to risk stratification activities where the outcome impacts the treatment the patient will receive. It may be advisable for any risk stratification to be reviewed by a clinician prior to any actions being taken.

5. Impact on Consent

The term “consent” has been used widely in the context of the common law duty of confidentiality when patient data is shared between organisations and was also associated with compliance with the Data Protection Act 1998. The term consent is also used for common law consent to treatment, which is an important part of medical ethics and for compliance with international human rights law. The mixed use of the term consent continues to cause confusion as we look to ensure GDPR compliance in clinical and medicines homecare services.

Common law confidentiality requirements are unaffected. This means that homecare providers do not need to change their current consent practices in order to comply with the GDPR, unless their organisation chooses to rely on GDPR consent as the legal basis for some of the lawful processing they undertake. NCHA recommends using different terminology to ensure patients understand the difference between common law consent to treatment and GDPR consent to processing of their personal data – the recommendation is to use the terminology “permission” for the former and to use the unqualified term “consent” only to mean GDPR consent.

The ICO recommends that if consent is difficult, as it is in clinical and medicines homecare services, organisations should look for a different lawful basis. There is a stricter interpretation of consent enshrined in GDPR. GDPR consent must be freely given, specific, informed and unambiguous and should not be a pre-condition of access to public services. This means that cases where the patient’s data must be held for clinical records or other regulatory purposes, consent is not an appropriate lawful basis for that data processing.

GDPR consent is reserved for truly optional elements of the clinical and medicines homecare service where it is solely the patient’s choice to participate or not e.g. patients signing up to...
participate in a pharma funded Patient Support Programme and/or where the referral to the clinical and medicines homecare service is not made by the clinician responsible for the patient’s care (see section 3.4) and/or participation in clinical trials.

Where GDPR consent is used as the legal basis for processing data there must be a clear statement of consent and/or a clear affirmative action by the patient – including specific informed consent to pass the data to any other data processor or controller especially if that data processor or controller will rely on that GDPR consent. If the patient withdraws consent or asks for this data to be restricted or deleted, it must be restricted or deleted (unless there is another justification under GDPR for continuing to process that data). If that data has passed to any other data controller, the patient must be notified and that data controller is also obligated to delete or restrict the data.

Consent provisions relating to children have not changed.

6. Lawful Basis for Data Processing in Clinical and Medicines Homecare Services

Within clinical and medicines homecare services, there must be an Article 6 lawful basis for the general processing of personal data. The Article 6 lawful basis for data processing is likely to vary depending on the circumstances of the service as outlined below.

In the majority of cases, the Article 6 lawful basis will be supplemented by the Article 9(2)(h)\(^7\) lawful basis for processing the special data relating to a patient’s health and demographic information. The same Article covers occupational health and personal data for employees providing the healthcare service.

Most lawful bases require that processing is ‘necessary’. If you can reasonably achieve the same purpose without the processing of personal data, you will not have a lawful basis. The ICO requires organisations to consider and document the lawful basis for processing at the outset and further recommends that “you should not swap to a different lawful basis at a later date without good reason”.

As clinical and medicines homecare services are multi-organisation services, it is important for the parties to agree which legal basis for data processing is being used and which organisation is the data controller at each stage of the homecare service so that information to patients is clear and consistent. Failure to reach agreement may expose all parties to claims of GDPR non-compliance evidenced by inconsistencies in the published Privacy Notices of the organisations.

6.1 For NHS Purchasing Authorities and Clinical Referring Centres

NHS England has advised that the Article 6(1)(e) (processing is necessary for the performance of a task carried out in the public interest.) will be the lawful basis that applies to NHS purchasing authorities and NHS clinical referring centres referring patients for clinical and medicines homecare services funded by the NHS under the clinical responsibility of an NHS Healthcare Professional. Public authorities are specifically excluded and may not use “legitimate interests” as a legal basis for data processing. Vital interests may only be used in

\(^7\) Article 9(2)h – “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 and safeguards referred to in paragraph 3”
life or death situations when other lawful bases are not applicable, so this is not appropriate for routine clinical and medicines homecare service delivery.

The NHS position in Scotland and Wales is being clarified.

6.2 For Non-NHS Clinical Referring Centres
Non-NHS clinical referring centres who refer patients to clinical and medicines homecare services are likely to lawfully process data on the basis of their contract with the self-pay patient or alternatively from their legitimate interest in providing healthcare to the patient under the clinical referring centre’s contract with the patient’s health insurer.

When providing clinical and medicines homecare services to non-NHS patients, it is advisable to check the lawful basis on which the clinical and medicines homecare referral has been made and resolve any anomalies that arise on a case by case basis.

6.3 For Homecare Providers
For NHS patients referred to receive clinical and medicines homecare services, homecare providers will routinely process personal information under the lawful basis of legitimate interest of providing the clinical and medicines homecare service to the patient following referral from the clinical referring centre. The reasons for this and circumstances where an alternative lawful basis may apply are outlined below. More than one lawful basis may apply to any given circumstance.

6.4 Legitimate Interest as the lawful basis for data processing
Homecare providers will have a “legitimate interest” in processing the patient data to deliver clinical and medicines homecare services to NHS patients, following referral from an NHS clinical referring centre.

For private patients, especially, where there is no direct contract with the private patient, the homecare provider will have a “legitimate interest” in processing the patient data to deliver the clinical and medicines homecare service which has been contracted with another third party e.g. when the homecare provider’s contract is with the patient’s insurance provider.

Homecare providers also have a “legitimate interest” in keeping patient and staff personal and health data relating to the provision of the clinical and medicines homecare services in case of personal injury or other claims which may arise many years after the services were provided.

Furthermore, using legitimate interests as the legal basis means that the personal and health data of patients provided by the NHS, may not be further processed without specific consent of the data subject and may only be processed by homecare providers for the purpose of providing that clinical and medicines homecare service and directly related activities. In particular, the patient data may not be used for electronic or telephone marketing as “legitimate interest” does not extend to any use which would otherwise require consent under the Privacy and Electronic Communications Regulations.

Further information and guidance, on how to perform a “legitimate interests assessment”, is provided by the Information Commissioner.⁸

6.5 Public task as the lawful basis for data processing
Whilst it would be expected that the lawful basis used by homecare providers would mirror that used by the NHS clinical referring centres and NHS purchasing authorities, public task is not available as a lawful basis for data processing by commercial organisations.

6.6 Vital Interest as lawful basis for data processing
Vital interests\(^{10}\) may only be used in life or death situations when other lawful basis are not applicable, so, whilst this may be appropriate in exceptional emergency situations, this is not appropriate for routine clinical and medicines homecare service delivery where the homecare provider also has legitimate interest in processing the patient’s personal and health data.

6.7 GDPR Consent as the lawful basis for data processing
GDPR consent is only applicable in optional and additional elements of a clinical and medicines homecare service such as a Patient Support Programme as discussed in section 2.

Optional pharma manufacturer funded Patient Support Programmes will rely on robust GDPR consent processes being implemented. In these cases, patients must give informed consent, having been informed how their personal data will be processed, by which organisations and that there may be elements of their personal data that are collected during the service, that must continue to be held and processed under another lawful basis including “legitimate interest” once the patient has participated in the Patient Support Programme (e.g. records of prescriptions dispensed, clinical procedures undertaken) and that this will impact their right to be “forgotten”.

6.8 Performance of a Contract as the lawful basis for data processing
The legal basis of performance of a contract may not be routinely used by homecare providers as the contract for the clinical and medicines homecare service is with the clinical referring centre or other purchasing authority or private health insurer and is not routinely with the patient (data subject).

For private patients receiving clinical and medicines homecare services there is a direct “self-pay” contract with the patient that provides the legal basis for data processing of accounting information Article 6(1)(b)\(^{11}\) in the performance of that contract.

6.9 Legal Obligation as lawful basis for data processing
Legal obligation, Article 6(1)(c)\(^{12}\), applies to copies of prescriptions dispensed, prescription book entries and records related to CQC registered activities. This would not cover all the information held and processed in the provision and monitoring of the clinical and medicines homecare service so would not be an appropriate lawful basis for routine processing of personal data within the clinical and medicines homecare service.

---

\(^{9}\) Article 6(1)(e) “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”

\(^{10}\) Article 6(1)(d) “processing is necessary in order to protect the vital interests of the data subject or of another natural person” and this cannot be achieved via another legal basis.

\(^{11}\) Article 6(1)(b) - “processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”

\(^{12}\) Article 6(1)(c) - “processing is necessary for compliance with a legal obligation to which the controller is subject”
6.10 Delivery Sub-contractors
Where a third party makes deliveries and/or collections of sealed consignments as part of the clinical and medicines homecare service, they should only have access to relevant personal information. Care should be taken not to disclose health information on labels and delivery documentation. The delivery organisation has a legitimate interest in using the delivery address, contact name and, where appropriate, contact phone number to make the delivery.

6.11 Clinical Sub-Contractors
The legal basis for data processing used by clinical sub-contractors will be similar to that used by the homecare provider.

7. Pseudonymisation and Anonymisation

Personal data anonymised in accordance with the principles of the ICO guidance on anonymisation\(^\text{13}\) is no longer regarded as personal data and therefore is not subject to GDPR requirements. GDPR clarifies that any pseudonymised data must be treated as patient identifiable data unless it can be proved that the information cannot be “decoded” to reveal patient identities by any originating organisation – not just the receiving organisation. Personal data may be anonymised by passing through several layers of pseudonymisation coding provided that there is no practical way that any organisation having access to the anonymised data could link the data back to identify the individual. If data is anonymised in this way the risk of the patient identity being revealed must be fully considered.\(^\text{14}\).

8. Breach notifications and fines

Where there has been a data breach, reporting to the ICO must occur within 72 hours of becoming aware of the breach. Failing to notify the ICO of a breach when required to do so can result in a significant fine of up to €10 million or 2 per cent of your organisation’s global turnover, whichever is the greater. The maximum fine for breaches in some cases will be €20 million or 4% of turnover.

It is important to have robust contractual provisions such that any organisation acting as a data processor that sustains a data breach must inform the data controller without undue delay as soon as they become aware. The data controller is responsible for the breach reporting obligations under the GDPR.

9. Data Protection Officer

Homecare providers process large amounts of personal data, including “special category” data, so each organisation must have a Data Protection Officer (DPO). The DPO for data protection is akin to the Responsible Person on a Wholesale Dealer’s Authorisation. The role can be internal or an external consultant can be appointed, but the person must be independent of the decisions made in relation to systems and data processing. GDPR includes some definitions of what independent means notably that ‘[the] DPO cannot hold a

\(^\text{13}\) https://ico.org.uk/media/1061/anonymisation-code.pdf

\(^\text{14}\) Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person (recital 26 Recital 26 of the European Data Protection Directive 95/46/EC).
position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case'.

The key requirements of the DPO role are:
- reporting to the highest management level of the organisation
- prompt involvement in all data protection issues
- supported by appropriate resources
- maintenance of expertise.

Further guidance is provided by NHS Digital.\textsuperscript{15}

10. Implementation of the General Data Protection Regulations in Clinical and Medicines Homecare Services

As clinical and medicines homecare services are multi-organisational services, it is imperative that the organisations involved are clear about the status of the other organisations and legal basis for data processing being used by their partners.

11. Data Mapping

\textsuperscript{15} https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/o/iga_-_guidance_on_the_gdpr_dpo_v1_final.pdf
12. Legal Basis for Data Processing

There have been discussions regarding the status of homecare providers as data controllers or data processors over many years and organisations have come to different conclusions. Whilst some homecare providers have signed Data Processing Agreements with individual NHS Trusts, all NCHA members currently designate themselves as data controllers and registered with the ICO under the DPA 1998 as organisations that hold sensitive personal data. It is now important to resolve this discrepancy in understanding so that homecare organisations (NHS Trusts and homecare providers) maintain compliance with GDPR and patients do not receive conflicting information.

The fact that one organisation provides a service to another organisation does not necessarily mean that it is acting as a data processor. It could be a data controller in its own right, depending on the degree of control it exercises over the processing operation.\(^{16}\)

A **data controller** determines the *purposes* for which and the *means* by which personal data is processed. So if the organisation decides ‘why’ and ‘how’ the personal data should be processed, it is a data controller.

Activities such as interpretation, the exercise of professional judgement or significant decision-making in relation to personal data must be carried out by a data controller.\(^ {17}\) It is important to remember that there can be multiple data controllers of the same personal information.

---


Following a recent industry workshop, the NCHA has developed the following position regarding the status of homecare providers alongside representatives from the NHS National Homecare Medicines Committee and data privacy specialists from NHS England.

The clinical referring centre retains clinical responsibility for the patient and is clearly the data controller for their patient record, patient referral /registration information and prescribing data.

At the point of referral, the clinical referral centre is the controller and the homecare provider is a data processor. The homecare provider remains data processor on behalf of the clinical referring centre until the patient is registered with the homecare provider. Once the patient is registered with the homecare provider, the homecare provider exercises professional judgement in the provision of the services to each individual patient. This means that the homecare provider has its own legal obligations to keep records and decides how and why data is processed during the delivery of the clinical and medicines homecare service to meet those legal obligations. The homecare provider therefore becomes a data controller as they manage the day to day service for an “active” patient.

Other reasons why it would not be appropriate for the clinical referring centre to be sole data controller for the entire service include;

- Information about the homecare provider’s staff who deliver the service to individual patients is inextricably linked to the patient’s clinical and medicines homecare service record.
- There are increasing numbers of cases of individual clinical and medicines homecare patients with complex conditions receiving clinical and medicines homecare services from different clinical referring centres.
- Rarely, patients disclose information to the homecare provider and specifically ask this is not shared with the clinical referring centre.

Whilst it is theoretically possible for a data processing agreement to be put in place detailing every possible data processing scenario and all record retention requirements, in practice, the burden of detailed data agreements between each homecare provider NHS clinical referring centre would be untenable. Furthermore, homecare providers cannot operate as data processors for many different data controllers, each of whom could issue legally binding instructions to the homecare provider causing unintended, but significant, patient safety consequences. So homecare providers must control “how” the data is processed within the context of similar services being provided to many different NHS clinical referring centres.

NHS clinical referring centres can be assured that patient identifiable data provided to the homecare provider, using the public task lawful basis for processing, can only be processed by the homecare provider for the “legitimate interest” of delivering the clinical and medicines homecare service, which the NHS has commissioned. Whilst legitimate interest is a wide category, the homecare provider can only use the personal data in ways that patients would reasonably expect and this test must be strictly applied where special data is being processed. In practice this means the patient’s personal data will only be used to provide the clinical and medicines homecare service as stated in the clinical referring centre’s clinical and medicines homecare service information and the homecare provider’s welcome pack. These documents are normally agreed between the parties during implementation of each clinical and medicines homecare service. Furthermore, the patient data may not be used for electronic or telephone marketing as legitimate interest cannot be extended to any use which would otherwise require consent under the Privacy and Electronic Communications Regulations.
GDPR enforces the principles of “purpose limitation” and “fair lawful and transparent processing” which puts requirements on all data controllers. It would be considered a new purpose should the homecare provider use NHS patient identifiable data, for any reason outside their legitimate interest in delivering of the NHS commissioned clinical and medicines homecare service. The patient would have to give GDPR consent for their data to be used for this new purpose unless there is another clear lawful basis for processing the patient’s data and that new purpose must not have unjustified adverse effects on the patient. Furthermore, under fair processing a homecare provider can only use NHS patient identifiable data to contact the patient to request consent for a new purpose where the patient might reasonably expect it. NCHA will strengthen the NCHA Code of Practice to ensure any new purpose secondary use or onward sharing of patient identifiable data is transparent with the data subject and the original data controller from whom the data was obtained.

NCHA agrees that within provision of clinical and medicines homecare services to NHS patients, data controllers must be registered and compliant with NHS Data Security and Protection Toolkit18.

14. Record Keeping

The GDPR includes requirements for accountability and evidencing compliance. There is a shift away from assumption of compliance with the regulations which is only tested when a breach occurs. With GDPR, homecare organisations must be able to produce records to show that the legal basis of data processing has been explained to the data subject and data security measures are in place and have been implemented in all individual cases. The phrase commonly used in pharmaceutical manufacturing is likely to apply going forwards - “If it isn't documented, it didn't happen”.

The majority of homecare patients have long term conditions, therefore clinical records for clinical and medicines homecare services need to be kept for 30 years according to the Records Management Code of Practice for Health and Social Care 201619. Clinical records for clinical and medicines homecare patients are embedded within the homecare service patient record, so there is a legitimate interest in keeping the full patient record for 30 years as it is too difficult to segregate historical patient data. Even if measures were to be put in place now to segregate that data in future, it is likely that the majority of the record would need to be retained.

18 https://www.dsptoolkit.nhs.uk/
15. Industry Level Recommendations

15.1 Work with NHMC to agree and document the legal basis of data processing in clinical and medicines homecare services for NHS patients as outlined in this paper.

15.2 Work with NHMC to define an industry template for data flows of patient identifiable information, data retention timelines and example data protection risk and impact assessments based on ICO guidance[^20] as outlined in this paper.

15.3 Resolve the proof of delivery (POD) process and remove the need for patient identifiable data in invoices.

15.4 Change terminology to “permission” for common law consent and use “consent” as an unqualified term only for GDPR consent.

15.5 NCHA should strengthen the NCHA Code of Practice to ensure any use or onward sharing of patient identifiable data is transparent with the data subject and the original data controller from whom the data was obtained.

15.6 NCHA will work with NHMC to perform a review of how the arrangements are working in practice under the GDPR after 12-18 months and will work together to find and implement solutions to any ongoing challenges that remain once the GDPR provisions are embedded in homecare organisations (NHS Trusts and homecare providers).

NCHA Position Statement 15 January 2019
IMPACT OF GENERAL DATA PROTECTION REGULATION IN CLINICAL AND MEDICINES HOMECARE SERVICES

References

General Data Protection Regulation (GDPR) guidance, NHS Digital
https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

This page includes links to guidance from the Information Governance Alliance.
- Frequently asked questions (updated regularly)
- GDPR: what’s new
- GDPR: implementation checklist
- GDPR: guidance on the Data Protection Officer
- GDPR: guidance on accountability and organisational priorities

Guide to the General Data Protection Regulation (GDPR), Information Commissioner’s Office

Data controllers and data processors: what the difference is and what the governance implications are, Information Commissioner’s Office


Guidance of GDPR Data Protection Officers - https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/o/iga_-_guidance_on_the_gdpr_dpo_v1_final.pdf

Acknowledgements

NCHA would like to thank Carol McCall for drafting this document and leading the multidisciplinary workgroup review and consultation. NCHA very much appreciated the assistance of NHS colleagues in developing this consensus position relating to the implementation of GDPR in clinical and medicines homecare services.

In particular, NCHA would like to acknowledge support received from Sean Kirwan, Senior Data Sharing and Privacy Manager, NHS England
Kiran Mistry, Data Sharing and Privacy Specialist, NHS England
Kevin McEvoy, Lead Policy Officer – Engagement (Public Services), Information Commissioner’s Office
Stacey Egerton, Senior Policy Officer – Engagement (Public Services), Information Commissioner’s Office
Susan Gibert, Chair National Homecare Medicines Committee
Joe Bassett, East of England Regional Homecare Specialist
Barry Moult, Former Chair of NHS Strategic Information Governance Network (SIGN)
### History

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Date</th>
<th>Reason for change</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft V1.1</td>
<td>First Draft for comment</td>
<td>9 March 18</td>
<td>New Position statement predates the coming into force of GDPR and the DPA 2018</td>
<td>Carol McCall</td>
</tr>
<tr>
<td>V1</td>
<td>Approved</td>
<td>26 Sept 18</td>
<td>New for circulation to Members and key stakeholders</td>
<td>Carol McCall, Kiran Mistry, Joe Bassett, Susan Gibert, Stacey Egerton</td>
</tr>
<tr>
<td>V1.1</td>
<td>Approved</td>
<td>15 Jan 19</td>
<td>Minor corrections prior to publication</td>
<td>Carol McCall</td>
</tr>
</tbody>
</table>

### Disclaimer

NCHA does not warrant or represent that the material in this document is accurate, complete or current. Nothing contained in this document should be construed as medical, commercial, legal or other professional advice. Detailed professional advice should be obtained before taking or refraining from any action based on any of the information contained in this document.