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

Frequently Asked Questions

Version 1.1

Dated 15 January 2019

This FAQ document supplements the NCHA Position Statement Impact of the General Data Protection Regulation in Clinical and Medicines Homecare Services (version 1.1 dated 15 Jan 2019).

Please note in order to aid reading, key sections have been identified. However, we advise readers to review all the questions and answers in their entirety as we have tried to avoid duplication of information across multiple answers.

Sections are as follows:

- General Questions
- NHS Questions
- Data Processor / Controllers Responsibilities
- Data Sharing Agreements
- GDPR Impacts for Manufacturer Funded Homecare Services
- Informed Consent
- Private Patients
- Record Keeping and Data Management
- Reporting Incidents and Breaches
- Right to be Forgotten

Public Domain

Disclaimer

General Questions

1.	Q	Does the guidance apply to the whole of the UK?
	A	The guidance has been developed in conjunction with NHS England. Representatives of Scotland, Wales and Northern Ireland are members of NHMC and have been involved in the consultations, although the guidance is currently only applicable to England.
2.	Q	Do you have an estimated time frame from NHS Wales, Scotland and Northern Ireland regarding when they will provide their positions on GDPR?
	A	NHS Scotland have just published their position on information sharing. https://www.informationgovernance.scot.nhs.uk/istresources/. The initial plan is to minimise the amount of work by having one agreement between each Homecare Provider and NHS Scotland, which should then be used for all Health Boards with minimal changes. This work is anticipated within the first half of 2019. We currently have no timescales for Wales and Northern Ireland.
3.	Q	What data is considered anonymous?
	A	Health and Social Care GDPR Working Group is currently preparing guidance on anonymisation and pseudonymisation of patient data. But in simple terms, any data that cannot be linked back to the data subject is considered anonymous. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.
4.	Q	What is the difference between an incident and a breach?
	A	Under GDPR, a breach, otherwise known as; "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. Article 4(12). GDPR commonly uses the term incident to describe a potential loss of personal data (e.g. a parcel containing medicines is delivered to the wrong address and not opened) and a breach to mean actual loss of personal data. In homecare services, an "Information Governance Incident" would include both GDPR Breaches and GDPR Incidents i.e. any loss or "near miss"/potential loss or unauthorised disclosure of personal data. Also see FAQ section on Reporting of Incidents and Breaches

NHS Questions

5.	Q.	Do NHS Trusts need to update their Privacy Notices, or is that something that only Homecare Providers need to do?
	A	All data controllers need to update their privacy notices with any new processing activity.
6.	Q.	When do NHS Trusts need to complete a Data Protection Impact Assessment (DPIA)?

	A	A DPIA is needed for any new processing activity which is considered high risk. In simple terms, NHS Trusts are often dealing with sensitive data which is considered high risk. If you deal with sensitive personal data with potential high impact, a DPIA will be needed.
7.	Q.	Should NHS Trusts have a Data Protection Protocol (DPP) in place and how does the DPP 'fit' within current contracts?
	A	Trusts must undertake a contract variation for any homecare contracts that are impacted by GDPR the next time the contract is renewed or updated to refer to the prevailing NHS Standard Terms and Conditions and an appropriately completed Data Protection Protocol. This may be undertaken at framework agreement level but in such cases each contracting authority would need to ensure this reflects their Trust's call-off service under that framework agreement. The new NHS Standard Terms and Conditions for Homecare Services will include the basic legal provisions required for GDPR compliance. These are due to be published in early 2019. Each new homecare service contract will then need a Data Protection Protocol to complete the contractual documentation set. NHMC is currently developing a template Data Protection Protocol suitable for use with NHS commissioned homecare services. Also see FAQ section on Data Sharing Agreements.
8.	Q.	Should my Trust Data Protection Officer (DPO) review and approve my homecare documentation and Data Protection Impact Assessments (DPIAs)?
	A	Normally a member of the Trust Information Governance team will suffice. A DPO can review DPIAs but cannot approve. They are only there to advise, and cannot determine data processing activities of the organisation.

Data Processor / Controllers Responsibilities

9.	Q.	Are community pharmacies data controllers of their pharmacy system records?
	A	When a professional and/or regulated activity takes place, the organisation with the professional responsibility to direct the purpose and means of the data processing activity (Article 4), is a Data Controller. In this example the community pharmacy is data controller for their own records of dispensing medicines and/or providing advice to patients.
10.	Q.	If a Homecare Provider is providing a basic dispense and deliver medicines service, are they the data processor or data controller? If there is a clinical or nursing element to the homecare service, what is the status of the Homecare Provider or sub-contracted Nursing Provider?
	A	As the Homecare Provider is dispensing medicines they would be a data controller in the same way a community pharmacy will be data controller for the patient records they generate.

		This means that Homecare Providers providing dispense and delivery service become data controllers for their record of that patient's data on first dispensing for each patient. A data processor does not direct the purpose and means of the data processing activity (Article 4), For clinical and nursing services, whilst each case must be assessed individually, an organisation that does not create their own further personal information, but simply processes the personal information provided by a data controller for the purpose determined by the data controller is likely to be a data processor. As a rule of thumb, Homecare Nursing Providers registered with CQC and undertaking regulated activity would be considered data controllers as they provide a professional service where they determine the purpose and means relating to their patient records of the regulated activities provided. For unregulated clinical and nursing services, the status of the organisations involved would need further individual assessment.
11.	Q.	Can a Homecare Provider or Homecare Nursing provider become data controller before the first dispensing of medicines for a newly registered patient?
	A	The Homecare Provider may become data controller at an earlier time if they provide a professional or regulated service in advance of the first dispensing. Examples would be a home visit by a nurse to assess risk and determine the suitability of the patient and their chosen location or self-administration training prior to dispensing.
12.	Q.	Can a pharma manufacturer be a data controller?
	A	A data controller is defined by the role and no different view can be taken. If you fall within the definition of Article 4, GDPR then you are a data controller. If an organisation provides a professional, regulated healthcare service directly to a data subject, that organisation generates personal information which they are responsible for directing the purpose and means of processing and that organisation is therefore a data controller. In funding a homecare service, the manufacturer determines the menu of services that will be offered to a cohort of patients, but does not normally determine which services are provided to individual patients and therefore does not determine the purpose and means of data processing. In a regulated Patient Support Programme or patient access scheme, identifiable personal information may be provided to the manufacturer who decides whether the supply of medicines can be made to an individual patient. An example would be thalidomide supply where the conditions of the Pregnancy Prevention Programme must be fulfilled. In these cases, the manufacturer may be designated as data controller for the patient records they generate. Data controllers holding or processing NHS Patient Data must comply with the provisions of the Data Security & Protection (DS&P) toolkit. All data controllers must pay a data protection fee to the Information Commissioner. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-fee/

13.	Q.	Are delivery companies such as third party couriers considered data controllers? Can you please explain the reasoning behind this view, as there is some difference in understanding between some couriers as they think they are data controllers, but we regard them as data processors.
	A	Where the courier is provided with the packages containing the dispensed products including name address and delivery schedule. There is an argument that couriers are data processors as they are not directing the purpose and means of data processing, but are acting on the instruction of the Homecare Provider who is the data controller. Deliveries are to be signed for, and if the delivery cannot be completed the Homecare Provider is notified and the package is then returned. Any issues are reported to the Homecare Provider who is responsible for communication with the patient. However, the ICO guidance para 33-39 clearly says - mail providers/couriers who do not make their own records of personal information, i.e. they just read the label on the letter/package, sort and deliver as per the label are neither data processors nor data controllers. - couriers who make records to support their delivery service are data controllers but only for the personal data they generate when making the delivery i.e. the courier's system records of consignee name, delivery address, sender contact name and address, their driver name who made the delivery and any records they make for proof of delivery e.g. name and signature of neighbour if named consignee is not available. The homecare data for which the courier would be controller is not health data as this (should) never includes health data, only sealed consignment delivery information. See Article 4 for the definitions.
14.	Q.	Occasionally, patients disclose information to the Homecare Provider and specifically ask that this is not shared with the clinical referring centre. In the case of safeguarding concerns, would you therefore suggest that we go through our own routes of risk management, completely independent of the clinical referring centre/NHS Trust?
	A	Yes. If the patient has asked for the data not to be shared, the Homecare Provider will have to perform their own safeguarding assessment to decide if the data should be shared despite lack of patient's consent using one of the other conditions under GDPR article 6, for example - legitimate interests. Fair processing notices will also need to be updated. Social Care Institute for Excellence provides useful advice here: safeguarding-adults does not want to share
15.	Q	Who needs to appoint a Data Process Officer (DPO)?
	A	Most Homecare Providers process 'large' amounts of special category data and need to appoint a DPO. NCHA Code of Practice will be amended to require all NCHA Members to appoint a DPO. Also, all public bodies need to appoint a DPO. Basically, if you fall within the FOI definition of a public body then you do or if you provide services to the NHS then you would.

Data Sharing Agreements & Contracts

16.	Q.	What Data Sharing Arrangements should be put in place between Homecare Providers and NHS organisations / NHS Commissioners?
	A	The new NHS Standard Terms and Conditions for Homecare will include the basic legal provisions required for GDPR compliance. These are due to be published soon. Each service will then need a Data Protection Protocol to complete the contractual documentation set. NHMC is currently developing a template Data Protection Protocol suitable for use with NHS commissioned homecare services.
17.	Q.	How long do we have to review contracts and ensure data sharing provisions are fully in place?
	A	The guidance sets out the timescales for compliance. It is envisaged that each time a new contract is entered into or an existing contract is renewed, the contractual documentation will be reviewed to ensure GDPR compliance, meaning all homecare contacts will be GDPR compliant within one contracting cycle.
18.	Q.	Are there any terms which are recommended as industry best practice in data sharing agreements between Homecare Providers and manufacturers, particularly around handling data subject requests?
	A	The Information Governance Alliance (IGA) will be publishing guidance in relation to data sharing agreements/ processing agreements in the new year. There is also some helpful advice on the ICO website.
19.	Q.	Can Homecare Providers process pharmacovigilance and/or Adverse Event/Reaction personal and special category data outside the EEA? The NHS Standard Terms and Conditions for Goods and Services currently says that this is not allowed.
	A	We understand the updates to the NHS Standard Terms of Conditions will confirm that the provisions of the DS&P Toolkit must be complied with.

GDPR Impacts for Manufacturer Funded Homecare Services

20.	Q.	How does GDPR impact Manufacturer Funded Homecare Services?
	A	A general principle of data sharing and data processing is that these activities must be transparent to patients and clinical referring centres. Organisations must agree who is the data controller and/or processor and Privacy Notices must be consistent to avoid inconsistent information being provided to patients. Privacy notice(s) must identify the data controller and give details of how the data controller will store and process the data they receive, who will have access to the data, its purpose and give details of any onward sharing of the data. Under GDPR, pseudonymised data is considered to be personal level data (unless it can be demonstrated that it cannot be "decoded"), so sharing and processing of pseudonymised data must also be transparent to patients. A generic statement is not sufficient. As each data controller has a duty to make their own assessment of GDPR compliance, Homecare Providers are concerned that legal advisors within manufacturers will take different views. NHS England have committed to

		support the NCHA establish a single view where possible and create a common approach.
21.	Q.	Where personal data is routinely shared by the Homecare Provider with the manufacturer, will it be regarded as best industry practice to provide a link to the manufacturer's privacy policy/Privacy Notice as part of the patient welcome pack?
	A	When using GDPR consent as the lawful basis of data sharing, the patient must have full visibility of what will happen to their data and with whom it will be shared and how it will be processed. Where patient identifiable data is routinely shared with the manufacturer, a multi-layered approach to patient information will be regarded as best practice including signposting to the manufacturer's Privacy Notice in the homecare service specific patient information. Where the data is shared with the manufacturer who is data controller, full privacy information should be provided to the patient. Where data is shared with the manufacturer as data processor, the Homecare Provider's privacy information should name the data processors who will receive the personal data and explain what processing will happen.
22.	Q.	Recent trends have shown that a number of pharmaceutical manufacturers (Marketing Authorisation Holders (MAHs) process sensitive personal data outside the EU. What safeguards and visibility should the homecare company have regarding processing that takes place outside the EU? We understand transparency requires the Homecare Provider to inform the data subject about processing outside the EU.
	A	If sharing personal data outside EEA, the risks and mitigations need to be noted in the Data Protection Impact Assessment (DPIA). Also, a data flow map needs to be drawn up to show the flows. Lastly, it is the data controller's responsibility to ensure that their data processors are adequately handling their data and that there are adequate safeguards in place. Finally, privacy notices need to be updated so data subjects are aware of who their data is shared with, how it's stored, etc. Binding Corporate Rules are used by multinational organisations based in several "adequate" countries. The definition of adequacy can be checked with the Information Commissioner's Office. Homecare Providers should be assured that manufacturers meet the requirements of the NHS DS&P toolkit before providing NHS patient identifiable data under any lawful basis other than explicit GDPR consent.
23.	Q.	How could Homecare Providers gain visibility of adequacy decisions and binding agreements, where the European Commission (the Commission) declares a country's data protection laws or a binding agreement (e.g. the EU-US Privacy Shield) suitable for transferring personal data (without the need for additional safeguards)?
	A	This will be on the ICO website, or by contacting the ICO for further information or https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

24.	Q.	What documentation needs to be retained by Homecare Providers, if any for the purpose of demonstrating compliance to GDPR regulations for data sharing with companies that process outside the EU?
	A	The Homecare Provider should retain ● Data Protection Impact Assessment (DPIA) highlighting risks and mitigations including assessment of adequacy of data sharing agreements/ binding corporate rules. ● Fair processing notices issued to ensure that data subjects are aware. ● Data flow maps showing the flows of data. ● Details of any consultation with ICO if considering sending data to a country outside EEA or not covered by the Privacy Shield or not considered adequate ICO.
25.	Q.	Can clinical homecare companies process pharmacovigilance (PV) and/or Adverse Event/Reaction personal and special category data outside the EEA? What would be the lawful ground for processing this data?
	A	We expect the new NHS Standard Terms and Conditions for Homecare Services to require compliance with the Data Security and Protection Toolkit. The regulatory requirements for PV reports are that they are anonymised. Patients must provide explicit GDPR consent for the inclusion of their identifiable data in PV and/or AE reports.
26.	Q	How will GDPR work if the patient contacts the pharma manufacturer directly to report an Adverse Drug Reaction or Event or complaint (i.e. incident)?
	A	Assuming the pharma manufacturer is not the data controller for the homecare service, the pharma manufacturer should provide their Privacy Notice and gain explicit consent from the patient to record, hold, process and share their personal information related to the Adverse Drug Reaction or Event with other relevant organisations. Assuming GDPR consent to proceed is given, following the Homecare C&I Guidance, the pharma manufacturer will agree with the other parties involved in the incident which organisation will be primary investigator and which secondary investigator(s). The primary investigator should be the most appropriate party to investigate the incident, determine root causes and co-ordinate reporting – this is unlikely to be the pharma manufacturer unless they are already a designated data controller for the homecare service.
27.	Q	Where data will be legitimately and lawfully shared with a manufacturer by a Homecare Provider, is it sufficient to inform the patient of that transfer and provide them with a link to the manufacturer's Privacy Notice or must a copy of the relevant Privacy Notice be provided in full? (e.g. as part of the patient welcome pack) Is this the responsibility of the manufacturer / marketing authorisation holder, if they are data controllers in their own right, to have the necessary safeguards in place to assure GDPR adherence?
	A	Homecare Providers should be assured that manufacturers meet the requirements of the NHS DS&P toolkit before providing NHS patient

		identifiable data under any lawful basis other than explicit GDPR consent. It is the responsibility of all data controllers to ensure GDPR compliance. If the manufacturer is processing data on behalf of the Homecare Provider and is acting as data processor it is sufficient to inform the patient and provide a link to the Homecare Provider's Privacy Notice where the relationship and data sharing with data processors are explained. If the manufacturer assumes data controller status for patient identifiable data, full Data Privacy information must be provided by the manufacturer and the lawful basis of the data sharing and data processing must be transparent to the patient and their clinical referring centre. Where appropriate, explicit GDPR consent should be gained and documented prior to sharing patient data with the manufacturer.

Explicit Consent

28.	Q	What action should be taken if explicit consent is difficult to obtain?
	A	ICO recommends organisations assess if another lawful basis for data processing is applicable to that data processing. In homecare services this must also consider the additional requirements for processing Special Category Data (Article 9).
29.	Q	Does using consent as a lawful basis for data processing give the data subject more transparency?
	A	No, the data subject must be informed how their data will be used and shared irrespective of the lawful basis. The only exceptions normally used in homecare services would be certain safeguarding situations or in the case of criminal acts. Details of the exemptions are here (GDPR Exemptions)..
30.	Q	How long does GDPR consent last?
	A	Where data processing is ongoing, it is recommended that consent status of each patient is reviewed periodically. The relevant Data Protection Impact Assessment should guide the frequency of GDPR consent review. Also, if any new processing activity takes place, then GDPR consent needs to be revisited.
31.	Q	When asking the patient for consent to share their data with the manufacturer of their medicine(s), does the Homecare Provider need to mention the name of the pharma company that may contact them for follow up information or can it be generalised by stating that the "pharma company "? The same would apply to the consent for the patient information that may be forwarded onto the regulatory authority as we would not be able to list them?
	A	You need to be specific when using explicit consent as a legal basis to share patient identifiable data. Using the terminology "the manufacturer of your medicine" could be appropriate in some limited cases but the patient may be taking several medicines. To maintain transparency, it is recommended that the organisations that will receive the patient data is/are named when GDPR consent to share data is requested.

		Regulatory authorities would also have to be individually named. However, regulatory authorities do not require patient identifiable information and anonymised regulatory reports are not subject to GDPR.
32.	Q	NHS commissions an oral medication homecare delivery service. Patients are informed about an add-on homecare service which supports adherence for which they can sign-up themselves if they wish. What lawful basis would apply?
	A	Legitimate interest only applies for provision of NHS homecare services by Homecare Providers where referral is from a NHS clinical referring centre using the public task lawful basis. The patient would need to give explicit GDPR consent for their personal data to be held and processed to provide this truly optional add-on service.

Private Patients

33.	Q	What is the legal basis for data processing for private homecare patients?
	A	Self-funding private patients will have entered into a contract with the Homecare Provider to pay for the homecare service and the personal data can be used to deliver against that contract as detailed in Article 6(1)(b). Where the privately funded homecare service is provided via a contract between the Homecare Provider and an insurance company or employer, the Homecare Provider has a legitimate interest Article 6(1) f in delivering the homecare services in accordance with the Homecare Provider's contract with the payer. Article 6(1)(b) is not appropriate as the contract must be with the data subject.

Record Keeping and Data Management

34.	Q	What additional restrictions are there for special category data including health data?
	A	In addition to the lawful basis of processing any personal data under GDPR Article 6, there are additional requirements for processing special category data including health data Article 9.
35.	Q	If homecare services are never activated for a patient following receipt of the registration information, how long should the Homecare Provider hold the registration information before deleting it?
	A	Retention of records is governed by the Records Management Code of Practice In the Code published in 2016, the archive record should be kept for a minimum of 2 years as an Event and Transaction record where "referral not accepted" or "requests for funding for care not accepted". Any rejected referral to the service record should also be kept on the originating service file. As a general guide in homecare services, the NCHA position statement indicates retention of patients who never became active for 6 years due to risk of contract claims and complaints, especially where the patient was accepted onto the homecare service.

36.	Q	How long do records need to be kept when Homecare Providers deliver multiple services to a single patient?
	A	If the patient data is not useful and does not relate to other services being provided, it should not be retained for longer than required for that service. However, in homecare services there may be justification, for clinical or other reasons, to retain the previous service data along with the patient record for the current service especially in the case of long term or recurrent conditions. Decisions relating to data retention should be justified and documented.
37.	Q	Is a Homecare Provider required to have a separate retention period for commercial records vs clinical records? If so, what data is regarded by the NCHA as clearly falling within the definition of clinical records? Would records of deliveries made (and therefore prescriptions fulfilled) count as clinical records?
	A	There is a clear differentiation between data kept and shared solely for financial purposes (e.g. invoice, POD, delivery address, proof of product and service delivery) and the patient's clinical record. The distinction between the clinical record and the associated administrative information gathered by the Homecare Provider in the course of providing the service is not so clear-cut. The definition will depend on the sensitivity of the medicines to mishandling and the complexity of the treatment pathway being followed. Records of supplies of prescribed and dispensed medicinal products and sterile medical devices including brand, quantity, batch and/or serial numbers, and date of supply would be considered part of the patient's clinical record.
38.	Q	Is it necessary to differentiate between clinical and financial data?
	A	There are different retention periods for financial data (e.g. purchase orders, invoices, proof of delivery) and patient clinical records. Where possible, the patient's clinical record should be kept separately to the administrative data relating to deliveries (e.g. designated delivery address different from the home address, contact details for carers). It is recognised that GDPR also applies to historical data. Many Homecare Provider systems were designed prior to GDPR regulations coming into force, so it may not be possible to separate the administrative data from the clinical record. Homecare Providers would have a legitimate interest in keeping administrative data for the same retention period as the patient's clinical record if it is not reasonably practical to separate that administrative data from the patient's clinical record. GDPR requires that GDPR compliance is built into systems going forwards so, when changes occur, change management processes should seek to ensure data sets are segregated such that anonymisation and/or pseudonymisation of personal data is implemented where appropriate and the relevant retention periods can be applied.
39.	Q	If a Homecare Provider passes data relating to patients to a manufacturer without the patient name, NHS number and contact information, but only with a unique patient ID which is held by the Homecare Provider and the Homecare Provider never shares the "key" to unlock the identity of the patient with the manufacturer (but the Homecare Provider has that key), is this personal data or not? Does it make a difference if other parties apart from the Homecare Provider (e.g. the NHS Trust) hold the "key". In this scenario, if this is <u>not</u> regarded as sharing personal data, is it the NCHA position that the patient should nonetheless always be made aware that the anonymised data will be shared with the manufacturer (given that there is a very

		slight risk that their data could be "unlocked" either by the Homecare Provider or by another party in future)?
	A	This would be fine if the degree to which the data may be linked back is minimised to near impossible without the key. But further guidance is coming from NHSE/ ICO. It makes no difference which organisation holds the "key". The important factor is the accessibility and security of the key. Where pseudonymised data is shared, it is always good practice to inform patients about all data sharing and to be transparent to ensure data subjects are made aware by the controller of all the data processing activities.
40.	Q	How do we inform existing patients of updates to Privacy Notices? Is it enough to include the Privacy Notice in the patient welcome pack and publish it on the organisation's website?
	A	Each organisation must assess the needs of the data subjects. The ICO favours a layered approach using patient leaflets, phone operators etc. Homecare organisations should not rely only on website information, as they cannot assume that everyone has internet access. Some NHS Trusts have sent letters and Privacy Notices to all patients, some have hand-outs available at key locations within the Trust, others signpost and provide links to their website. There is no consistent model and any channel can be used as long as patients are informed. The NHS would like to standardise the approach, but this will take time.

Reporting Incidents and Breaches

41.	Q	How does the reporting of an incident and a breach differ?
	A	All Information Governance Incidents and Breaches should be reported using the organisation's internal Complaints and Incidents procedures in accordance with the RPS Homecare Handbook Appendix 19: Further guidance on managing complaints and incidents within homecare services. If there are multiple data controllers involved in an incident, the primary and secondary investigators should be agreed and clearly identified in reports. For GDPR compliance, the Information Governance Toolkit has been updated into the Data Security and Protection Toolkit. The criteria for assessing whether a breach must be reported have changed and the new guidance can be found here https://www.dsptoolkit.nhs.uk/Help/29. The updated criteria are based on the likelihood of the breach having occurred and the severity of the impact on the data subject(s). If an actual breach is not reported to the ICO, the organisation's Information Governance Incident report should include justification based on the level of risk (likelihood and severity) in accordance with the DS&P Incident Guidance. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. The ICO has produced a guide which may be found on its website. If an organisation decides not to notify individuals of a breach, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a

		risk to rights and freedoms. The ICO has the power to compel organisations to inform affected individuals if it considers there is a high risk. Organisations should document their decision-making process. Minor breaches must be logged. They can be logged/ reported on the Data Sharing and Privacy toolkit, but this should not be used in place of the organisation's local incident management process. It is solely for the purposes of reporting to the relevant regulatory authority. If there are multiple data controllers involved in an incident, only the primary data controller must report a breach, however, other secondary data controllers may have their own regulated reporting requirements. When secondary investigator(s) report the same breach, the two reports need to be clearly cross referenced to avoid duplication of investigation efforts and double counting of breaches. Further guidance on Primary and Secondary investigators and reporters for incidents can be found in the RPS Homecare Handbook Appendix 19.
42.	Q	What are the requirements for reporting of a Breach?
	A	It is the data controller's responsibility to report any breaches meeting the reportable criteria given in https://www.dsptoolkit.nhs.uk/Help/29. Breaches must be reported to the ICO within 72 hours of the breach becoming known via the Data Security and Protection Toolkit. Reporting on the Data Security and Protection Toolkit will automatically notify the ICO if the incident meets the reporting criteria and an email confirmation should be received by the reporting organisation that the ICO has been informed. The incident record on the DS&P Toolkit can be edited until it is reported to the ICO. Once reported to the ICO, the DS&P Toolkit entry is "locked" and updates should be sent directly to the ICO. In the case of significant breaches (loss of data), it is recommended that the homecare organisation also directly notifies the ICO of the incident including the DS&P report reference to ensure compliance with GDPR Article 33 which requires reporting of a breach within 72 hours. Where multiple data controllers are involved in an incident, more than one of the organisations may be required to make a regulatory report. It is also possible that the breach is an incidental part of a wider patient safety incident where only the secondary investigator is required to make a regulatory report. In all case liaison between the data controllers is important to ensure robust reporting without unnecessary duplication.
43.	Q	Can Homecare Providers rely on the NHS Toolkit making a data breach report to the ICO or should reportable data breaches be also made directly to the ICO? If a direct report must also be made, what is the best practice to avoid confusion/duplication of workload at the ICO, within Trusts and Homecare Providers?
	A	Reporting on the Data Security and Protection Toolkit will automatically notify the ICO and an email confirmation should be received by the reporting organisation that the ICO has been informed. In the case of significant breaches (losses of data) it is recommended that the homecare organisation also directly notifies the ICO to ensure compliance with GDPR Article 33 which requires reporting of a breach within 72 hours.

44.	Q	When a patient dies, can this be reported to a manufacturer using patient identifiable data?
	A	Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR. However, any duty of confidence established prior to the patient's death must be respected. Normal procedures for anonymising and/or pseudonymisation of patient data should be followed for PV reports to avoid distress to the deceased's carers and relatives. ICO guide-to-gdpr-v1 (page 11)
45.	Q	If there is a data breach involving a third party (e.g. a courier delivers a prescription to the wrong address), does this need to be reported by the party responsible for the breach (e.g. the courier) or by the Homecare Provider?
	A	A courier is likely to be data processor for the organisation that dispensed and despatched the consignment. The incident needs to be reported immediately by the courier to the Homecare Provider who is the data controller. It is the data controller's responsibility to report a breach to the ICO.

Right to be forgotten

46.	Q	How do you manage the right to be forgotten?
	A	Where there are regulations which require the organisation to keep records and this overrides the data subject's right to be forgotten, the patient should have been informed of the legal basis being used for processing their data via the Privacy Notice. If a patient requests to be forgotten, the organisation must explain any data they are keeping and/or continuing to process and the reasoning behind their decision.
47.	Q	A patient asks the Homecare Provider to be forgotten. The Homecare Provider has previously used the lawful basis of consent to pass patient identifiable data to the manufacturer (Marketing Authorisation Holder). Does the manufacturer have to delete the patient's data?
	A	Each organisation that has received that patient's data from the Homecare Provider has to be notified of the patient's request to be forgotten. Data processors must act on the instruction of the data controller from whom they received the information. Where the patient consented to data sharing with another data controller, the patient must have been fully informed before the original data sharing occurred. The additional data controller must have asked for and received specific consent for their additional data holding and/or processing and must have provided their own Privacy Notice to the patient. The data controller(s) for the patient identifiable information must decide whether the data they hold should be deleted and each data controller must inform the patient of any data they will continue to keep and/or process including the lawful basis for their decision.
48.	Q	If a data subject sends a request to be forgotten to a Homecare Provider, does the Homecare Provider have to inform the recipients of pseudonymised data who do not have the key to "unlock" the data?

	A	Pseudonymised data is considered personal data under GDPR, so recipients of pseudonymised data would need to be informed unless that data can be reclassified as anonymised. There are circumstances when this type of data may be defined as anonymous and therefore not subject to the provisions of GDPR. NHSE is developing further guidance on pseudonymisation and anonymisation of NHS patient data.

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 guidance relating to the implementation of GDPR in clinical and medicines homecare services.

In particular, NCHA would like to acknowledge support received from

Kiran Mistry, Data Sharing and Privacy Specialist, NHS England

Shaid Hussain, Senior Data Sharing & Privacy Manager, NHS England

Susan Gibert, Chair National Homecare Medicines Committee

Joe Bassett, East of England Regional Homecare Specialist

History

Version	Status	Date	Reason for change	Author(s)
V1	Approved	26 Sept 18	New	Carol McCall Kiran Mistry Susan Gibert Joe Bassett Shaid Hussain
V1.1	Approved	15 Jan 19	Minor corrections prior to publication	Carol McCall

NHS Publishing Reference 001086