Information sharing protocol across secure and detained settings

NHS England and NHS Improvement

Information sharing protocol across secure and detained settings

Publishing approval number: **000388**

Version number: V.0.11

First published: July 2019

Updated: (only if this is applicable)

Prepared by:

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact england.healthandjustice@nhs.net

Contents

1 Glossary of terms

Item	Description
BMA	British Medical Association
CCG	Clinical Commissioning Group
DHSC	Department of Health and Social Care
DPA 2018	Data Protection Act 2018
FOI 2000	Freedom of Information Act 2000
GMC	General Medical Council
HMPPS	Her Majesty's Prison and Probation Service
NOMS	National Offender Management Service
HO	Home Office
IG	Information Governance
IRC	Immigration Removal Centre
ISP	Information sharing protocol
MHT	Mental health trust
MoJ	Ministry of Justice
PHE	Public Health England
PPO	Prisons & Probation Ombudsman
PSD	Personal Sensitive Data
SCH	Secure Children's Home
STC	Secure Training Centre
YJB	Youth Justice Board
YOI	Young Offender Institution

2 Introduction

This national **Information sharing protocol** (referred to as the ISP) is an overarching agreement between the parties to regulate the sharing of specific Personal Sensitive Data (PSD as defined in the Data Protection Act 2018 and General Data Protection Regulation 2018. It provides a framework for assuring the safeguarding of PSD by all parties.

Adherence to this ISP does not provide legal indemnity from the Data Protection Act 2018 (DPA), General Data Protection Regulation 2018 (GDPR) or any other legislation nor should its use ignore Caldecott guidelines which must be adhered to as required. It serves only to record the data to be shared, benefits expected, etc, and to demonstrate that the parties have been mindful of, and documented compliance with, relevant Acts, Codes of Practice and Guidance.

This Protocol is designed to be an overarching agreement to confirm and not supersede locally managed and developed agreements.

This Protocol specifically refers to the treatment of individual patients by multiple providers, across the health and secure sectors.

3 Scope

3.1 Legal scope

For information to be processed lawfully, the processing must comply with GDPR Article 6, and the corresponding inclusion within Data Protection Act 2018[1].

For healthcare in the secure and detained estate relies on Article 9(2)h as follows:

> *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***

Additionally within DPA (18) further restrictions apply:

'(1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.'

[Ref of para in DPA]

The list of health professionals is defined in the DPA18 in Section 69[2] and as modified by subsequent legislation.

The DPA 2018 requires that organisations follow 6 principles. These are detailed in the body of this Protocol and at **Appendix A**. In terms of the sharing (or disclosure) of data regarding individuals, the DPA 2018 requires that data are processed only for specific purposes and that data are not shared in ways incompatible with those purposes.

All organisations processing personal data are required to inform data subjects (patients) of the uses of their data, these public notices are called Privacy Notices, which must include the purposes for processing of personal data, and the retention periods for that personal data, and who it will be shared with.

[1] The relationship between GDPR and DPA (18) is beyond the scope of this paper. However, the legal position of data protection legislation within the UK will not significantly change with/without "BREXIT".

[2] http://www.legislation.gov.uk/ukpga/1998/29/section/69

Additionally, the legal requirements around confidentiality are based on previous court cases decided by judges; hence, it is referred to as 'common', 'judge-made' or case law. The law is applied by reference to previous cases decided in the law courts. Generally, all sharing of information requires the consent of the individual, be it implied or explicit, should it leave the care of the individual responsible for it, but the concept of the care team means that it is entirely legitimate for the information to be shared for the purposes of:

- The direct care (diagnosis/therapy/treatment) of the individual.
- In relation to safeguarding.
- Where there is a risk of serious harm to others.

This is supported in guidance from key clinical professional bodies such as the General Medical Council and Royal College of Nursing.

In respect of clinician to clinician information sharing The British Medical Association has provided guidance which describes a 'legitimate relationship' between the person providing treatment and the patient.[3] The guidance refers to principles for sharing information for direct patient care and in paragraph 6 states:

> *'Healthcare teams should only be able to view the records of patients with whom they have a direct clinical relationship. This means that the patient must be registered on the system of the organisation which wishes to view their record, for example as a result of referral. It should not be possible for one organisation to view all of the records of another organisation.'*

The principle of the legitimate relationship and functional purpose are key to this Protocol, and to ensuring that patients' right to privacy is respected.

The Protocol also supports the seven Caldicott Principles:

1. Justify the purpose
2. Don't use patient confidential data unless it is absolutely necessary
3. Use the minimum necessary patient information
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

[3] http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records/principles-for-sharing-local-electronic-patient-records-for-direct-patient-care

Recognition of Principle 7 includes the need to share data to deliver the best outcomes for patients. This duty to share supports the specific operational circumstances within the experience of the secure estate.

Where patient autonomy is constrained by the secure environment it is necessary that those functions usually undertaken by Carer, parent/guardian are properly transferred to those staff (healthcare and security staff) within the secure estate workforce who are able to support and assist the patient.

3.2 Organisations party to the Protocol

The organisations party to the Protocol are detailed in Appendix D.

Guidance on identifying the status of organisation as Data Controller, Processor, or Joint Controller has been followed in creating this Protocol (see **Appendix A)**.

> Note that these designations **only** relate to data shared under this Protocol and the ensuing data flows as detailed in **Section 6**. Each party must be registered with the Information Commissioners Office (ICO) as a Data Controller in its own right and be assured of compliance with relevant legislation. Additionally, any NHS Service provider must register with NHS Digital and submit satisfactory annual Data Security and Protection Toolkit compliance. Details of relevant SIRO, Caldicott Guardian and IG Leads should also be recorded on the relevant NHS Digital registration log. The full details of the organisations and their designated officers, responsible for data protection in association with this Protocol, are listed in **Appendix B**.
>
> Each party must ensure that the specific department or team involved in the data sharing is clearly identified. Other personnel from the party's organisation not formally identified are not authorised to have access to the data. Internal organisational access to shared information must be limited to those that have a legitimate and approved need to see those data. Internal technical and organisational measures taken to prevent unauthorised access to shared data and information covered by this protocol must be documented within the policies and procedures of the organisation concerned.

Each organisation is responsible for ensuring that all staff who operate under this Protocol are fully aware of their duties, either via training or other communicated means, and are operating in compliance with the Protocol at all times. This Protocol should be read in conjunction with the Prison Health Access Agreement, which sets out the expectations on organisations on specific elements of Information Assurance which will apply and includes the requirement to be subject to independent audit in order to provide assurance.

4 Purpose of information sharing

NHS England Health and Justice commissioning operations are responsible for the commissioning of healthcare across England for secure and detained settings. This organisational responsibility is overseen by 4 (7 from 1st April 2019) field force areas across England and directly supported through Health and Justice locality leads. In addition NHS England holds Partnership Agreements between Her Majesty's Prison and Probation service (HMPPS, as an Executive Agency of the Ministry of Justice), NHS England and Public Health England (PHE), the Department of Health and Social Care (DHSC) and the Ministry of Justice (MoJ) for services across the adult secure estate; the Home Office Department of Immigration Enforcement, PHE and NHS England for Immigration Removal centres; and the MoJ, PHE and NHS England for YOI's and Children's secure settings. Any additional commissioning responsibilities NHS England subsequently take on will be managed within one of these agreements.

The National Operating Model for Offender Health Care sets out NHS England's responsibilities for the on-going provision of services. This includes:

- An open and transparent approach, sharing information freely wherever appropriate, and lawful;
- Contributing to reducing violence, in particular by improving the way the NHS shares information about violent assaults with partners, and supports victims of crime; and
- Combine local knowledge with shared national values and behaviours with information flowing between local and national teams contributing to the key outcomes and improvement areas, namely:
    - Reducing health inequalities;
    - Ensuring services are integrated; and
    - Reducing health risk factors.
    - Safeguarding and reducing risk of harm to self and others.

There are significant and compelling reasons why a national Protocol to support local ISP's is required. Notwithstanding all the factors above there is, as a regular feature across PPO and coronial reports into deaths within the secure estate, a lack of appropriate and timely information flow between health staff as well as between health and detention staff which has been found to be contributory to self-inflicted deaths.

NHS England through the commissioning and contracting process is responsible nationally for the design, development and provision of ICT equipment, connectivity and software to manage healthcare across the secure and detained estate (excluding currently police custody settings). This national approach ensures that all healthcare delivery within the secure setting is consistent and compatible between sites and services. The single information architecture provided by NHS England permits s standard approach to data collection and processing and ensues

consistency in definition and processing of information throughout the service on a national basis.

Each provider is mandated by contract to provide a service and, within that contract, must adhere to terms and conditions around Information Governance and data processing commensurate with NHS policy.

NB: The clinical system currently employed across the secure and detained environment has some weaknesses in its ability to appropriately control access to individual elements of the patient record, and will be shared by the multiple providers listed in **Appendix A**. Discussions between NHS England, the System Author and the ICO are ongoing. This Protocol has been created, in part, to address the expectations for each party in using the clinical system, and to manage the areas of the system they are authorised to access and view.

This Protocol is owned by the organisations who are signatories listed in **Appendix B**. The management and change of the Protocol is organised by the respective organisational information governance teams. Any change or amendment of the protocol will be agreed by all parties and authorised jointly prior to changes being implemented.

5 Justification for sharing

In order to achieve high quality healthcare delivery within the secure and detained estate there needs to be appropriate and timely collaboration between the providers of both health care and the secure environment. The sharing of information must be done in a lawful and transparent manner and be for the benefit of a patient's health. For this objective to be achieved with efficient and effective operational delivery within the secure environment all parties must recognise the value of information sharing and understand the importance of being able to do so appropriately, lawfully and confidently.

The provider types included in the health care team include:

- Acute Trusts
- General practice
- Community health providers
- Mental health providers
- Optometrists
- Dentists
- Pharmacists
- Substance misuse teams
- Out of hours providers
- Any qualified providers – clinical or non-clinical services

The provider types in the secure estate included:

- Detention staff (across prisons, YOIs and IRCs)
- SCH and STC staff

- Education staff
- Ancillary support staff

The second report by the National Data Guardian highlighted the vital importance of information and data sharing within health and social care processes. The provision of information supports both the quality of care and the delivery of positive outcomes for patients. Individually clinicians need timely, complete and accurate information to ensure efficient diagnosis and treatment of patients.

Information sharing supports the efficient on-going care provided to patients and prevents repeat testing or the need for patients to repeat detail when seen by differing teams within a care pathway. This exchange of information is most important when a patient is concurrently managed by both healthcare staff and secure estate staff. Both staff groups have a common interest in the wellbeing of patients and the reduction of risk and the prevention of harm. The existence of a joint duty of care provides a common channel for the exchange of data between the two agencies.

The National Data Guardian notes in her second report that patients and the public expect that clinicians will share data across organisational boundaries in the best interest of patients and to ensure the continuity of any care provided. Likewise, the sharing of information in the best interests of the patient can be a justification to share. Reports from Death in Custody Reviews and Coronial report frequently identify lack of shared information as contributory to fatal incidents within the secure estate.

National Data Guardian Report (Caldicott 2) 2013:
Most people who use health and social care services accept and expect that doctors, nurses and other professionals will need to share personal confidential data if they are going to provide optimum care. People get frustrated if they have to answer the same questions repeatedly as they move along a care pathway. It may be good professional practice for a clinician to check an item in a medical record by asking the patient to expand on a previous answer. However, it is not good practice for important information to be missing from the record. Patients and service users want the professionals to act responsibly as a team.
Fiona Caldicott, NDG

Within the Health and Justice system the joint responsibility for the care and welfare of patients between a number of providers can be a complex process. For the management of risk, and for welfare, it is important to recognise that the sharing of data, information, and “soft intelligence” by all those agencies involved can be both necessary and desirable. Data Protection legislation (including EU General Data Protection Regulation and Data Protection Act 2019) recognise the need to protect highly sensitive data, Inc. personal health data. However, legislation specifically recognises the need for sharing of data for ”the provision of health or social care or

treatment or the management of health or social care systems and services" [GDPR Article 9(2)h]. The Information Commissioners Office (ICO) also supports the sharing of information for direct care.

Information Commissioners Office
In the healthcare sector, patient data is held under a duty of confidence. Healthcare providers generally operate on the basis of implied consent to use patient data for the purposes of direct care, without breaching confidentiality.

ICO Health GDPR FAQ

Therefore, the shared responsibility for the care and welfare of patients does provide a legitimate purpose to share appropriate clinical data between the direct care team and the detention staff to facilitate the ongoing care and treatment of the individual. Any service provider must ensure that information exchange is proportionate, necessary and minimalised, but sufficient for continuity of care to be provided to the patient.

6 Principles for sharing the data

6.1 Sharing within the clinical team

Healthcare organisations will have access to the clinical data of all patients currently within the secure estate clinical arrangement. This includes:

- Patient demographics
- Summary of clinical conditions
- Medications
- Interactions and recorded consultations
- Test results
- Dental history
- Optometry history
- Substance misuse
- Safeguarding (risk to self and/or others).

The system allows controlled access to all this data to all those granted access. Fair processing of personal and sensitive data as required by the Data Protection Act 2018, requires that an individual should expect that their data will be used in a certain way. It would be outside this expectation, and therefore a potential breach of the Act, for a clinician to purposefully access information about another entirely separate clinicians' treatment of the patient. For example, whilst full clinical information may be readily available to the Optometrist, it does not necessary follow that individual recorded consultations with the Mental Health professional should be accessed (see also Caldicott Principle 2, above).

Authorised users should therefore not access the information about an individual, even if the system allows it, without the consent of the individual and without considering whether the individual would expect that access to be made, unless there is a compelling and defensible reason to do so.

The system records all interactions and keeps a full audit trail. The audit trail will be regularly monitored for appropriate access and users will be required to justify that access if necessary. It is within an individuals' rights, and enshrined in the NHS Constitution, to be given information about who has had access to their record, and with whom it has been shared – GDPR Article 12.

6.2 Sharing out of clinical team

This Protocol relates to the principles of sharing information from the clinical team for health and for non-healthcare purposes, and details the conditions under which it can be shared for this purpose.

Sharing information out of the clinical environment can be justified with ligament interest and defined purpose. Hence it would be appropriate to share information from clinical team to detention staff where this is necessary for treatment and diagnosis, or where this was necessary for the administration or management of healthcare services. This could include clinical appointment details to ensure that patients are able to attend consultation/therapy with clinicians.

6.2.1 Safeguarding

Safeguarding is a term used in the United Kingdom and Ireland to denote measures to protect the health, well-being and human rights of individuals and populations, which allow people — especially children, young people and vulnerable adults — to live free from abuse, harm and neglect. Many of these safeguarding interventions are subject to legislation; official guidance and all are party to professional standards and competencies.

Within the secure environment responsible staff ideally focus on empowerment, protection, prevention, proportionate responses, partnership and accountability to safeguard vulnerable individuals. This approach to care requires that both healthcare and detention staff adequately share data to ensure that protection can be provided.

6.2.2 Administration and management of systems/services

Controllers that are part of a group of undertakings or institutions affiliated to a

central body may have a legitimate interest in transmitting personal data within the group of

undertakings for internal administrative purposes, including the processing of clients' or

employees' personal data.

Derogating from the prohibition on processing special categories of personal data

should also be allowed for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services,

> *GDPR (2018) Recital 53*
>
> *"Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system*

6.2.3 The risk of harm to the individual or others

The DPA 2018 makes it a requirement to process data only if certain conditions are met. While it allows processing to protect the vital interests of the patient or another person (in Schedule 1 part 2 paragraph 19), under the duty of confidentiality, confidential patient information should not generally be shared when a patient objects – even if a healthcare professional believes sharing information would be in the patient's best interests. If it is intended to override the patient's wishes, then it will be necessary to find a legal basis to do so.

Note that nothing should delay release of the information if a person is likely to cause immediate serious harm.

All organisations should be mindful of the 7 Caldicott Principles when deciding to share any information with other health care professionals or with detention staff.

6.2.4 Record management

It is expected that all organisations will enter consultations and interactions with patients on the clinical system being used in the secure and detained setting making that clinical system the principle patient record.

All clinicians should treat the information they hold about individuals as confidential and it should only be shared or accessed where there is a legitimate relationship with the patient for the specific clinician concerned.

Similarly, it is good practice and expected in the use of the system that clinicians will discuss with patients the areas of their record they are about to access in support of their care.

It is a requirement that all temporary and agency staff have been vetted to NHS Standards by their supplying organisation before being allowed to work in the prison health system.

7 Organisational and technical measure

7.1 Access control

Requirements for users to be given access to the clinical system are set out in a separate access agreement document.

The separate access agreement documents the appropriate management and procedures that should be in place for granting access.

7.2 Security of information

It is expected that each organisation keeps information secure in line with the Data Security and Protection Toolkit requirements to Level 2 and other law and guidance as previously outlined.

Specific areas of Information Security to be in place at each organisation are specified in the separate access agreement document.

7.3 Consent

Generally, staff can rely upon implied consent when sharing confidential patient information for direct care purposes. The signatory organisations owning this Protocol will each have their own explicit guidelines regarding consent in order to assist staff in their decisions about when explicit consent may be required from patients – for purposes other than direct care - prior to information sharing taking place.

Explicit consent may be verbal, and it is accepted good practice to record this in the system when given. It is good practice to continue to check with a person their position in respect of consent remains.

The signatory organisations have organisational constitutions which detail how their client group can be informed as to how their records and personal information will be safeguarded and maintained, and the length of time for whish such records will be retained.

Consent must be obtained to enable records to be shared and the matrix embedded in **Appendix C** details where organisations can rely on implicit or explicit consent to share the information with other healthcare professionals within the prison clinical environment.

It is within an individuals' rights to be given information about who has had access to their record, and with whom it has been shared.[4]

7.4 Circumstances where information may be shared without consent

There are certain circumstances where consent can be set aside:

Where not disclosing might cause serious harm to the physical or mental health or condition of another person

- If instructed by a court order or if there is a statutory requirement to disclose (e.g. to protect another person from serious harm or to support the investigation/prosecution of serious crime)
- Where the patient is judged by a clinician to lack capacity to make a decision themselves healthcare staff should follow the guidance set out in the Mental Capacity Act Code of Practice[5] when deciding whether or not they can share confidential patient information
- Where the public interest served by disclosure outweighs the public interest served by protecting the patient's confidentiality AND the public interest served by providing a confidential service.

8 Monitoring and audit of the Protocol

Each organisation will have a data management group whose responsibility it will be to ensure data management is appropriate and lawful.

[4] http://www.nhs.uk/choiceintheNHS/Rightsandpledges/NHSConstitution/Pages/Overview.aspx

[5] https://www.gov.uk/government/publications/mental-capacity-act-code-of-practice

The NHS England management group (see section 4) will be responsible for managing audit and reporting for access to records in the clinical system and for the appropriate use of patient information.

The named organisations will undertake spot checks of their own adherence to this Protocol either directly or through monitoring of standards referred to within. Any resulting report of checks related to this Protocol can be reasonably requested by any other party to this Protocol.

The Commissioner may request of any organisation party to the Protocol any relevant confirmations of standards such as the information governance training compliance of staff with or intending to be granted user accounts for the shared systems.

The Commissioner will audit against the standards outlined in the Prisons Access Agreement.

9 Subject access and Freedom of Information

9.1 Subject access and information rights requests

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) provide the right that a person may request and have copies of any personal information held about them by any organisation.

The following process will be followed in responding to a subject access request from an individual patient:

If the request is made to an individual Data Controller, that Data Controller is authorised to provide copies to the patient as they see fit, but ONLY for the information held in the record for which their organisation has made an entry.

If the request is made for the whole record, this request must be passed immediately to the nominated person in the Health team, who will collate the information and request confirmation from each Data Controller that they are content for the information to be released to the data subject. It is generally good practice to inform the data subject if any information has been withheld from the request; in most circumstances the only information that should be considered exempt from a Subject Access Request is information that identifies a third party.

Each organisation should ensure that all staff are aware that there are differing procedures for Subject Access relating to the disclosure of prison health information as above.

Incorrect entries in the clinical record

Where a Data Subject has asked for a correction to be made to their record, it will be the responsibility of the organisation receiving the request to amend their own records as they see fit and in line with their own professional guidelines.

If the request relates to an entry made by another organisation or clinician, then no amendment must be made, and the request must be notified to that organisation ***without delay***. The individual making the request for amendment must also be informed as to the transfer of their request, and the reason for the transfer, as the requirement to reply within a legislative time-frame, starts counting down from the time of the receipt by the applicable data controller, not the delivery of the request.

All such amendments must be recorded in the clinical system as appropriate and the management group can be used as a final decision maker by reference to the nominated representative.

The clinical system may allow entries in records, or entire records, to be deleted without an audit trail being retained. **UNDER NO CIRCUMSTANCES** should any individual or organisation delete entries or a record without the written permission of the management group.

9.2 Freedom of Information and Environmental Information Requests for information

Individual organisations are responsible for their own Freedom of Information or Environment Information requests as appropriate.

Where a request is received for the secure and detained health service, this must be forwarded immediately to the nominated person on the management group to be processed.

10 Research

Where parties wish to undertake research where health information is required this will only be permitted with the agreement of the NHS England management group and an application must be made prior to any research taking place. Other organisations management group will have to ratify research projects where data pertinent to their roles and responsibilities is requested.

11 Summary Care Record

Currently, the prison clinical system will not link to the Summary Care Record systems.

However, should the system become linked, all patient wishes regarding the Summary Care Record must be respected and the relevant codes added to the clinical system where required. For more information please refer to the following websites:

Summary Care Record

http://www.nhscarerecords.nhs.uk/

12 Serious Incidents Requiring Investigation (SIRIs)

The Protocol recognises the importance of managing and responding to losses or near misses relating to patient information.

As well as following their own internal procedures (i.e. as set out in the Information Governance Toolkit), all potential near misses or losses of PSD must be reported to the nominated person immediately upon discovery.

The nominated person will keep an appropriate log and be responsible for ensuring that appropriate steps are taken to mitigate against further data breaches.

All organisations are required to comply with any investigation into the cause of a loss or near miss and to take part in mitigating actions to prevent recurrence.

13 Court orders or other lawful basis

Where an organisation receives a court order to release patient confidential information regarding information it has recorded as part of its service, nothing in this Protocol prohibits the release of that information. Staff need to take care when responding to a mandatory request for confidential patient information that they only supply the information that is necessary and proportionate for the purpose (e.g. do not provide a copy of a patient's entire medical record if you have been requested to provide information about a particular incident or episode of care).

14 Retention and disposal of data

Each party to the Protocol will apply where necessary, relevant regulations to the retention, storage and disposal of records, only keeping data for as long as necessary in relation to original purpose(s) for which it was collected. Retention periods will be set by NHS England in collaboration with partners and to meet the legal obligations of the Act, balanced by the requirement to support medico/legal and accountability.

Each party to the Protocol will have appropriate records management procedures in place to ensure that they have taken account of and follow the guidelines for records retention contained in Records Management: NHS Code of Practice Part 2, Annex D1 and any subsequent updates[6]

Under no circumstances should data be deleted from any system without the proper authorisation having been first gained from the management group (please also see section 6.8).

15 Management of the Protocol

15.1 Protocol management

NHS England is responsible for the approval, maintenance and review of this Protocol, in conjunction where necessary with the signatories within **Appendix B**

15.2 Retention of signed copies of the ISP

The signatories are responsible for maintaining signed copies of this Protocol.

15.3 Nominated contact point

Each party to the Agreement will identify a nominated contact point. Contact details of the nominated contact point are to be detailed in **Appendix B**.

[6] http://systems.hscic.gov.uk/infogov/links/recordscop2.pdf

Where nominated contact points change, the appendices will be updated as soon as possible and communicated to the other parties.

15.4 Amendments to the Protocol

Proposed amendments to the Protocol must be tabled at the management group, and a revised Protocol produced and signed as agreed.

15.5 Review of the Protocol

The Protocol will be subject to regular formal review, following changes to law, ethics & policy in relation to the security and confidentiality of information or on a bi-annual basis led by the management group.

15.6 Monitoring of Protocol

Each organisation signatory to this Protocol is responsible for ensuring full compliance of all staff within their organisation to the terms and conditions of this Protocol. Any identified areas of non-compliance must be forwarded to the nominated person on the management group.

15.7 Termination of the Protocol

This Protocol will run alongside the Commissioning contract and will be considered in force under the same terms as that Protocol.

From the agreed termination date, no further transactions will occur or be attempted on the relevant system.

Appendix A: Relevant law and guidance regarding Data Protection

Note: The Data Protection Act 2018 and GDPR were implemented from 25 May 2018. The implementation of GDPR significantly alters the data protection legislation and the overall environment within which this Protocol is delivered.

The principles enshrined within the Data Protection Act 2018 are described below.

Data Protection Act 2018 6 Principles

The Data Protection Act 2018 lists the data protection principles in the following terms:

1. Personal data shall be processed lawfully, fair and transparent and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 9 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 10 is also met.
2. Personal data shall be obtained on any occasion must be specified, explicit and legitimate and any personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for the purpose for which it is processed
6. Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

Further information and guidance can be found on the Information Commissioners Website at:

http://www.ico.gov.uk/for_organisations/data_protection.aspx

Further guidance in a range of areas for health and care organisations can be found at:

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

Who is a Data Controller?

Further guidance is available on the ICO website at http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-controllers-and-data-processors-dp-guidance.pdf

Note: Additional guidance relevant for GDPR should be considered during any review of this Protocol

1. The Data Protection Act 2018 defines a data controller as:
    a. "… a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".
2. It is important to establish whether or not someone is a data controller because it is data controllers who are required to comply with the Data Protection Principles.
3. A data controller must be a "person" i.e. a legal person. Whilst this may be an individual, e.g. a sole trader, it more generally refers to organisations such as NHS Trusts and other corporate and unincorporated bodies of persons.). "The NHS" or "The Health Service" are not legal entities and therefore cannot be data controllers.
4. Data controllers of personal data are those that determine the purposes for which that personal data are, or will be, processed and the way in which that personal data are, or will be, processed. The Commissioner's view is that the determination of the purposes for which personal data are to be processed is paramount in deciding whether a person or body is a data controller.

Who is a Data Processor?

8. The concept of „data processor" is also relevant, if only to eliminate it from consideration. This is defined in the Data Protection Act 2018 in the following way:

> **"**Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller."

9. The 2018 Act introduces specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors. The

data controller retains full responsibility for the actions of the data processor. The key obligation is that:

> "the processing must be carried out under a contract-
>
> > i) which is made or evidenced in writing, and
> > ii) under which the data processor is to act only on instructions from the data controller"

10. Whilst NHS bodies may enter into arrangements with organisations that function as data processors, and some may host information services that process data for others, they do not otherwise act as data processors themselves in respect of NHS data for other NHS bodies or the DH. Similarly, whilst DH consults with NHS bodies it does not generally act as a data processor on their behalf.

Further information and guidance on data protection

http://www.ico.gov.uk/for_organisations/data_protection.aspx

Appendix B: Parties to the Information sharing protocol

The following organisations are party to this Protocol:

Organisation name	Department or team	Data Protection Designation (controller/joint /processor)

Appendix C: Consent and legitimate relationship matrix

Typical patient information sharing consent form:

This form asks for your signed consent to contact certain people or agencies who may be involved in planning your care whilst in prison and on your release.

You should be aware that information may be disclosed in the following circumstances whether you consent or not: if the safety and security of other patients, staff or the wider community is compromised by not revealing information; if you are at risk of self-harm; or if there are any concerns under the Children's Act 1989 e.g. a child's welfare may be of concern.

There may be others who are not listed, however, we would make every attempt to inform you before we shared any information.

Relevant organisations	Yes	No
Health professionals		
PNOMIS		
NDTMS		
CRC NPS		
Psychology programmes		
Safer custody team		
Adults and children's social care		
Family		
Personal officer		
Police		
Prison escort		
CPS		
Defence legal representative		
MDT		
Research		
RECONNECT		
In the event a psychiatric report is requested, I give consent for the appointed psychiatrist to have access to my medical records		

I give consent for my medical information to be shared with my registered GP or other community prescriber to enable them to provide me with medical treatment after my release.

This form asks for your signed consent to contact certain people or agencies who may be involved in planning your care whilst in prison and on your release.

You should be aware that information may be disclosed in the following circumstances whether you consent or not: if the safety and security of other patients, staff or the wider community is compromised by not revealing information; if you are at risk of self-harm; or if there are any concerns under the Children's Act 1989 e.g. a child's welfare may be of concern.

There may be others who are not listed, however we would make every attempt to inform you before we shared any information.

I give permission for any member of the healthcare staff to request information from, or to provide information to the people or agencies about me listed overleaf.

I understand that I do not need to give consent again in order for this information to be passed on and shared between agencies, however the issue of consent will be raised periodically throughout my treatment interventions to ensure it is still valid.

I understand that this information is being shared with a view to ensuring and assisting in the continuity of my care. I am aware that I can withdraw my consent to this information being shared with any or all of these agencies at any time.

I have been told that where I have not agreed to my information being shared with and between any of these agencies this will not prevent me getting support that I need but understand that it may delay the process.

I have been told that all agencies listed above will respect the confidentiality of any information about me and that individuals will only share this information within their organisation, except for the purpose of ensuring my continuity of care.

I have understood the above, and consent for the healthcare staff to disclose medical information as indicted above. I also understand that this may be without my consent for reasons explained.

Patient name: …….

Patient signature: ……..

Patient number: ……..

Date:

Healthcare personnel:

By countersigning this form, you are confirming that in your view this consent is capacitated.

Healthcare staff name: ……..

Healthcare staff signature: ……

Date: ……

*Are there any exceptions to the above list that you do not wish us to share your medical information with? For example, if you ticked 'family' but there are particular family members you do not want us to share this information with.

Appendix D: Organisation sign off sheet and designated officers

The Caldicott Guardian or Senior Information Risk Owner **must** sign on behalf of each organisation. [The Protocol must have been reviewed by the relevant management groups in the organisation]

Original forms will be kept by the management group, copies should be kept by each organisation.

Organisation	
Name:	
Address:	

Caldicott Guardian/ SIRO name	
Caldicott Guardian/ SIRO Phone and email	
CG/SIRO signature	
GDPR Data Protection Officer	
Data Protection Contact (name, phone and email)	
Key Contact (name, phone and email)	