

Data Privacy Impact Assessment for SystmOne – HTML Record Access

Contents

Document History	2
Glossary	3
1. Purpose of Document	4
2. Need for DPIA.....	4
3. Information Flows and Description of Processing	4
Processing operations and purposes of processing (Article 35 (7)(a) GDPR)	5
4. Identify Privacy, Related risks and Solutions.....	6
5. Other Mitigations.....	14
Rights of Data Subjects.....	14
Rectification and erasure (Articles 16,17 and 19 GDPR).....	14
Restricting the processing of personal data (Articles 18, 19 and 21 GDPR)	14
Access to data (Articles 15 and 20 GDPR)	14
International Transfers	15
Data Retention	15
6. Actions and sign off.....	15
Appendix A – Controls within the HTML Records integration	17
Appendix B - Summary of Processing Operations	17

Document History

This section should only be used when a new version of an existing document is created. Newer versions should detail which sections have been amended/added.

Version	Review date	Changes
1.0	1st May 2018	
1.1	12th June 2019	Made the document more 'generic' as it was previously written for specific integrations but now covers any HTML Records integration.

Glossary

Term/Abbreviation	What it stands for
EHR	Electronic Health (and where applicable social care) Record(s)
GDPR	General Data Protection Regulation
eDSM	Enhanced Data Sharing Model
DPA	Data Protection Act (1998) or any subsequent applicable legislation
EHR	Electronic Health (and where applicable social care) Record(s)
GDPR	General Data Protection Regulation
ICO	Information Commissioners Office
IGSoC	Information Governance Statement of Compliance
N3	the connection to the national broadband network for the National Health Service (NHS), which such broadband network connects all NHS locations and employees across England
NHS	National Health Service
NHSD	NHS Digital
NHSE	NHS England
PIA	Privacy Impact Assessment
PIs	Private Items
RA	Registration Agent
RBAC	Role Based Access Controls
Sharing-In	the viewing of the EHR which has been set for Sharing-Out, by a healthcare provider on the basis of explicit or implied consent
Sharing-Out	the making available of the EHR, which includes personal and sensitive data, to other healthcare providers on the basis of explicit or implied patient consent
SystmOne Override	the viewing of the EHR which has not been set for Sharing-Out, by a healthcare provider on the basis that the patient now explicitly consents to the EHR retrieval or due to safeguarding concerns.

1. Purpose of Document

This Privacy Impact Assessment (PIA) has been written by TPP to assist in improving the design of functionality within its software, SystmOne, and to ensure that its software can be used by Data Controllers in a manner, which allows for compliance with the Data Protection Act 1998 (DPA) (to be updated by the 2018 Act) and the General Data Protection Regulation (GDPR). Personal sensitive/special data is processed by TPP and its software allows for electronic health (and where applicable social care) records to be shared between multiple organisations (involved in the direct care of patients) using another system.

Individual Data Controllers using SystmOne should create their own Privacy Impact Assessments, seeking the views of Data Subjects or their representatives and taking into account the data they hold, local and organisational processes and their obligations as Data Controller. The below assessment can be used as a basis for a PIA or as a supplement to any existing PIA.

2. Need for DPIA

SystmOne is provided to the NHS by TPP under a number of contract and framework mechanisms. SystmOne currently holds over 47 million EHRs including sensitive personal data (Article 9 and Article 10 GDPR). TPP acts as the Data Processor under contracts with the Data Controllers or their representatives. The processing is therefore on a large scale (Recital 91 GDPR) and could concern vulnerable data subjects (Recital 75 GDPR).

Furthermore, if the processing is wholly or partly performed by a Data Processor, the Data Processor should assist the Data Controller in carrying out the DPIA and provide any necessary information (Article 28(3)(f) GDPR).

HTML Records integration creates flows of data outside SystmOne (both directions). Therefore, we carried out the assessment in this document to examine any risks and their respective mitigation.

3. Information Flows and Description of Processing

SystmOne is a comprehensive EHR that supports clinicians, administrators and social workers to provide health and social care in the NHS, including providers commissioned and paid by the NHS, by Local Authorities, and providers commissioned and paid for by the Police and Crime Commissioners under the current arrangements for care in the Health and Justice System.

SystmOne already has a model in place for sharing the EHR between multiple organisations using SystmOne called the enhanced data-sharing model (see the eDSM enhancements PIA). Third party clinical systems will also have their own sharing models in place.

The HTML Records integration provides for the sharing of patient EHRs between different providers on different clinical systems within the health care estate subject to controls. Depending on the Third Party system, the records will come from a variety of care settings (e.g. Hospital, GP Practices, Community Care). List of care services that can use this integration from TPP is shown in the next section. The integration will allow for a view of the EHR only. This will support clinical decisions. The integration will not allow for the receiving organisation to update or amend the details within the provider EHR.

For a detailed description of the necessary controls that need to be enabled to allow for data to be shared between the SystmOne organisation and another organisations using the integrations please see the attached diagram below and Appendix A – Controls within the HTML Records integration:



HTML Records
integration controls

Additionally, the embedded functional guide offers detailed guidance on how the integration functionality operates



SystmOne-HTML
integration training

Processing operations and purposes of processing (Article 35 (7)(a) GDPR)

SystmOne stores over 47 million EHRs across a variety of health settings – see below. The system allows for health professionals with appropriate controls and access rights to view EHRs from other clinical systems that are designated to be shared between Data Controllers and equally, EHRs can be shared out from SystmOne to other clinical systems.

Some of the EHRs will contain sensitive information such as medical diagnoses and associated information. The integration is designed to allow for any organisation that is involved in the direct care pathway of the data subject to be able to access the patient EHR where the Data Controller has allowed this to happen.

TPP shall not engage another Data Processor without prior specific or general written authorisation of the Data Controller (Article 28 GDPR).

Care Services using the integration between SystmOne and Third Party systems.

- GP practices
- Community services such as district nurses, rehabilitation centres, telehealth and diabetes services
- Child health services that undertake scheduling of treatments such as vaccinations
- Urgent care organisations such as Minor Injuries Units and Out of Hours services
- Community hospitals
- Palliative care hospices and community services
- NHS Mental Health trusts
- NHS Hospital trusts
- Accident and Emergency departments
- Care Homes
- Social Care – registered and regulated professionals within social care organisations co-ordinating care (not social care providers)

Types of data subject

Any individual attending any of the above care services who could include;

- Children
- Vulnerable adults
- Individuals sectioned under the Mental Health Act (MHA)
- The elderly

Types of data

- Special/sensitive data
- Personal data

A summary of the Processing Operations for the integrations is displayed in the table at Appendix B below.

4. Identify Privacy, Related risks and Solutions

SystmOne has always provided a mechanism to share the EHR for direct patient care (to other SystmOne organisations), and many health communities have adopted the product for that feature. More recently, there has been a requirement to share EHRs outside of SystmOne and into other clinical systems.

It is self-evident that there exists the need to balance the benefits to the individual of sharing their EHR and the risk to the Data Controller. Due to the nature of the NHS - that it is a distributed service across the country, which can be accessed by any citizen anywhere at anytime - it may benefit the individual if the EHR were available for use at any of those locations, no matter which clinical system is being used, by the staff member providing the care.

For processing of health data by the NHS to be lawful, the Data Controller must have satisfied at least one condition for processing from both Article 6 and Article 9 of the GDPR.

The Data Controller must decide which condition they are relying on.

In order for the processing to be deemed fair and lawful, the Data Controller must provide the citizen (data subject) with a clear and comprehensive understanding of how their data will be utilised and shared outside of the recording organisation. This must be within the citizen's reasonable expectation. The combination of controls for the Data Controller together with controls for the data subject is to support this balance and ensure EHR availability when and where the data subject expects and wants.

The various controls, outlined within this DPIA (see Information Flows and Description of Processing and within Appendix A – Controls within the HTML Records integration below), must be considered with reference to the data protection principles but ultimately each Data Controller can decide whether they will adopt the functionality for the integrations in conjunction with their data subjects. SystmOne contains security controls that are compliant with GPsOC and NHS national framework standards. SystmOne is also ISO27001 accredited. The integrations do not alter the underlying security of the system. They do, however, greatly enhance both the Data Controller and the citizen's ability to control access to their EHR.

SystmOne users have the controls detailed in the documents embedded above - Information Flows and Description of Processing and described in Appendix A – Controls within the HTML Records integration in place that will prevent data being shared inappropriately.

DPA/GDPR Principle / Article at risk	Privacy Issue / Risk Source / Threat	Risk to Data Subject	Risk to Data Controller	Associated organisation / corporate risk	Solution (Article 35(7)(d) and Recital 90)	Result	Evaluation including necessity and proportionality assessment (Article 35 (7)(b))
Principle 1 / Article 5 (a) – Data must be processed fairly and lawfully and in a transparent manner in relation to individuals	Insufficient information and knowledge on record sharing for GPs and patients.	Not aware of when or where data is being processed - data disclosed beyond expectation.	Failure to fair process - not aware of when or where data is being processed.	Patient complaint	1.Ensure all parties have accurate and contemporaneous documentation in plain English to support their obligation (decision to share or not). 2.Provide suitably worded privacy notices. 3.Publicity campaign for patients via leaflets/posters; online guidance and multi-media displays of data flows. All of which can be accessible to Data Controllers to display in organisation where patients attend (including website). 4.Accessible audits of record access and sharing preferences. 5.Ensure contract drafting reflects roles of Data Controller and Data Processor. 6.A SystmOne user screen that lists all non-SystmOne organisations that have been configured to share data with	1./2. Assuming a suitably worded privacy notice can be drafted using comprehensive guidance distributed then the risk is substantially reduced. A level of risk remains of notice/documents becoming outdated. 3. Increased patient awareness of how data is shared for healthcare provision. 4. Greater transparency of EHR transaction; staff activity and reach of shared record. 5. Separation of roles made clear in contractual arrangements increasing understanding of obligations required to fulfil. 6. Organisations have control over who information is being shared with and to which clinical systems – control over the data flow.	Combined with the Data Controllers/subjects ability (if desired) to control which organisations can see their data via sharing lists the mitigations significantly reduce any risk in unfair processing. The benefits of sharing the EHR and retaining the freedom for the citizen to permit access to their record wherever they receive care outweigh the risk. Outcome: Risk is significantly reduced - Minimal risk - Accepted

These instructions are correct at the date of writing. For further assistance, consult the SystmOne Online Help.

Principle 1 / Article 5 (a)	Inability to control who can access the EHR and illegitimate access to EHR resulting in modification or deletion of data.	Inability to control who access their EHR	Not aware who has access to the data	Patient complaint	1. The caring organisation needs to decide which organisations they want to share data out to. 2. The Third Party System organisation needs to have a sharing agreement set up in their system with the SystmOne organisation for information to be shared. 3. Audit shows when and who have accessed the EHR.	1&2. This is a point-to-point sharing model, giving the data controller more control over who is allowed to access data their data (patient records). 3. Clear audit allows the users to check that no illegitimate access to the EHR has been performed and where there has been any illegitimate access, the caring organisation can re-examine the organisations they have set up to share data out to.	The ability to control the list of caring organisations who have access to the data, combined with the use of audits significantly reduce any risk in the inability to control who has access to the data. Outcome: Risk is significantly reduced - Minimal risk - Accepted
Principle 2 / Article 5 (b) – Personal data shall only be obtained for one or more specified and lawful purposes and shall not be further processed in a manner that is incompatible with the purpose; further processing for archiving purposes in	No new purposes are introduced.	No new risks identified	No new risks identified	No new risks identified	No new solutions needed – Data Controllers instruct TPP as Data Processor and the Data Controllers decide the legitimate basis for processing.	No new purposes are introduced.	No new risks identified

the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes							
Principle 3 /Article 5 (c) – Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed	The integration permits access to the complete EHR held on the respective data controller's system(with the exception of data recorded from the SCR exclusion set).	Beyond expectation - would not expect certain details to be revealed to the accessing individual/organisation.	No control over level of detail that can be accessed.	Patient complaint	1.Ability to mark items as private in the EHR. 2. Possibility that a centralised process could be implemented to determine which roles/users can access which items of data. 3.An exclusion list set out by the NHS England has been implemented to hide sensitive data.	1. Marking items as private allows both the Data Controller and data subject the ability to prevent certain data items being shared. 2. A central process would be useful for consistency across the profession but it does not exist and, if possible, it would take a very long time to implement. It would require all NHS organisations to operate in the same way, which is not feasible due to factors such as size of the organisation and location. 3. Data considered to be sensitive has been included in the SCR exclusion set, and will be hidden when the EHR is accessed.	The clinical risk to individuals of important health and social care decisions being made on incomplete or inaccurate information (especially in terms of unscheduled care) balanced with the mitigations, the ability to mark items as private and those mentioned in terms of principle 1; and the presence of the exclusion list in terms of principle 3 - will support privacy adequately and is justification for this balanced approach. Outcome: Risk remains – Minimal risk - Accepted

These instructions are correct at the date of writing. For further assistance, consult the SystemOne Online Help.

Principle 4 / Article 5 (d) – Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay	No change to data accuracy is introduced.	No new risks identified	No new risks identified	ICO intervention; BMA complaint; Patient complaint	No new solutions needed – see Other Mitigations below.	n/a	n/a
Principle 5 /Article 5 (e) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are	Excessive data may be retained for an inappropriate period in multiple locations.	Risk the data is open to more vulnerabilities if it is stored in multiple locations and is more difficult to monitor.	Excessive data retention	ICO intervention; BMA complaint; Patient complaint	1. The integration provides a view of the EHR when the record is retrieved but this does not persist.	1. The view of the EHR allows clinicians at an organisation to make an informed decision regarding the treatment of the patient with all available health and social care information at the time of the consultation.	The clinical risk to individuals of important health and social care decisions being made on incomplete or inaccurate information (especially in terms of unscheduled care) together with the controls required to allow the integration justifies the need to allow another organisation a view of the record at the time they require it but no longer. There is no need to persist the data in both systems as queries can later be made

These instructions are correct at the date of writing. For further assistance, consult the SystmOne Online Help.

processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals							with the provider system if required. Outcome: Minimal risk - Accepted
Principle 6 – Personal data shall be processed in accordance with the	No new risks identified	No new risks identified	No new risks identified	No new risks identified	No new solutions needed other than those mentioned above regarding data subject control over lists of organisations to share to and request to mark items as private.	As above.	As above.

These instructions are correct at the date of writing. For further assistance, consult the SystemOne Online Help.

rights of the data subject							
Principle 7 / Article 5 (g)– Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Inadequate controls preventing inappropriate access.	Risk of 'bad actor/rogue user' accessing their data.	Risk of 'bad actor/rogue user' accessing their data – mistaken or inappropriate access.	Patient complaint	1. Ability to restrict the 'pool' to fewer organisations via sharing lists mentioned above. 2. The integration is restricted to only viewing the EHR; the individuals accessing the data have no way of destroying or damaging the data accessed. 3. The user accessing the EHR shared via the integration must be logged on with a Smartcard and have appropriate access rights for registering patients and viewing the EHR.	1. Data Controllers should configure the 'pool' to only those organisations they are happy to share with and therefore they are aware of potential access. The Third Party systems mandate that a data sharing agreement is in place before a share can occur. 2. The fact that viewing is the only action allowed to be performed with patient's EHR being accessed means that no loss, destruction, or damage can be caused to patient data. 3. Trusted RBAC Agents must allocate users of the clinical systems permissions to access the clinical system and they grant rights based on their role at an organisations to a Smartcard for their use only. A PIN must be entered to access the system.	Combined with the registration process (patient must be registered for care at the accessing organisation), RBAC controls (for registering and accessing) and other deterrents such as professional codes of conduct, the common law and audits, the mitigations when applied by the Data Controller significantly reduce the risk of the 'bad actor/rogue user'. Therefore, the privacy risk is justified by the desire for an EHR to be available wherever the data subject attends or desires. The absence of ability to amend or delete data accessed brings no risk of accidental loss, destruction, or damage to personal data. Outcome: Minimal risk - Accepted

These instructions are correct at the date of writing. For further assistance, consult the SystemOne Online Help.

Principle 8 – Personal data shall not be transferred to a country or territory outside of the European Economic Area	No transfer of data outside the EEA is introduced.	n/a	n/a	n/a	n/a	n/a	n/a
---	--	-----	-----	-----	-----	-----	-----

5. Other Mitigations

Rights of Data Subjects

Rectification and erasure (Articles 16,17 and 19 GDPR)

To be carried out by the Data Controller (e.g. GP) ***unless assistance is needed from the Data Processor (TPP)***.

Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data. Where such a request is made, we shall assist the Data Controller where necessary, *unless there is an exemption*, to rectify the personal data without undue delay.

Data subjects have the right, *in certain circumstances*, to request that the Data Controller erases their personal data. Where such a request is made and assistance is needed from the Data Processor, TPP shall erase the personal data without undue delay if:

- (a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- (b) the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data is being processed and there is no other legal basis for the processing;
- (c) the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims;
- (d) the data subject objects to the processing of their personal data for direct marketing purposes;
- (e) the personal data has been unlawfully processed;
- (f) the personal data has to be erased for compliance with a legal obligation to which we are subject; or
- (g) the personal data has been collected in relation to the offer of e-commerce or other online services.

It is important to note that the purpose of the integration is to share health and social care records for the sole purpose of the provision of direct care by Data Controllers, who are themselves professionals in these fields, and so it is unlikely that the above scenarios will be applicable. Any risk is low.

Restricting the processing of personal data (Articles 18, 19 and 21 GDPR)

Data subjects have the right, *unless there is an exemption*, to restrict the processing of their personal data if:

- (a) the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;
- (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) we no longer need the personal data for the purposes we collected them, but they are required by the data subject for the establishment, exercise or defence of legal claims; and
- (d) the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

Access to data (Articles 15 and 20 GDPR)

Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs).

TPP, as Data Processor, will assist Data Controllers, to respond positively to subject access requests (replying via the same method as the request – paper, email etc.), as quickly as possible, and in any event within the **30-day**

time limit. Whilst individuals have a general right of access to any of their own personal information which is held, we will be mindful of those circumstances *where an exemption may apply*.

International Transfers

Unless otherwise stated, TPP do not process Personal Data outside of the European Economic Area (or any country deemed adequate by the Commission pursuant to Article 25(6) of Directive 95/46/EC) without the prior written consent of the Data Controller; and the following conditions are fulfilled:

The Data Controller or the Data Processor has provided appropriate safeguards in relation to the transfer;

- the data subject has enforceable rights and effective legal remedies;
- the Data Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
- the Data Processor complies with reasonable instructions notified to it in advance by the Data Controller with respect to the processing of the Personal Data.

Data Retention

TPP does not undertake any automatic data destruction. Any data destruction will only occur under the direct instruction of the Data Controller.

NHS patient records are covered by the Records Management Code of Practice for Health and Social Care 2016, which is classified as a guide to the requirements, since requirements come from many sources. Health records in SystmOne are more complex as many of them exist in a shared state, so although the organisation reviewing their retention process may no longer have a legitimate relationship with the patient, the record that organisation created is in use by others in the NHS and is of clinical relevance.

This situation will become increasingly widespread as EHR interoperability is established in the NHS, where a complete record will be assembled by calling all the components of the record that exists. It may not be in the best interest of the patient to have components of their records destroyed due to a retention schedule. It is, however, necessary for organisations to have clear records management codes in place (the FOIA and the DPA have records management codes of practice that recommend the systems and policies that must be in place to comply with the law). Most guidance revolves around *minimum* retention schedules. SystmOne EHRs contain multiple types of records (e.g. specimens and samples, integrated records, controlled drug regimes, child school health records inter alia) that cannot be separated as the code implies.

Deceased Patient Records

Recital 27 of the GDPR states that the regulation does not apply to the personal data of deceased persons. Any requirements for these records will be derived from the NHS code of practice, medico-legal requirements and adherence to the duty of confidentiality. TPP does not undertake any automatic data destruction for deceased patients.

TPP provides the Data Controllers with a draft/model Exit Policy containing options for data archiving and deletion. It is expected that Data Controllers will choose the most suitable option for their purposes and instruct TPP accordingly at this point the Exit Policy will become final.

6. Actions and sign off

The following actions will be ongoing and required by Data Controllers using the integration:

- Review of all training guides and support documents produced by TPP to support the integration.
- Refresh on all privacy notices produced by organisations using SystmOne.

This document will exist as a working document and will be kept under review to ensure that SystmOne provides the necessary controls for Data Controllers to maintain compliance with the DPA/GDPR.

This document will be made available to SystmOne users within SystmOne.

These instructions are correct at the date of writing. For further assistance, consult the SystemOne Online Help.

Appendix A – Controls within the HTML Records integration

- The ability to record an implied consent to share information in, the data subjects' explicit consent to share information in or a dissent to share in; The ability to record an implied consent to share information out, the data subjects' explicit consent to share information out or a dissent to share out.
- Organisational access to the integration is only available where the organisation has a N3/HSCN connection granted by NHS Digital.
- The ability to restrict record access to a particular staff member at an organisation.
- Individual access to the integration is controlled by a logon with access rights granted by the appropriate authority.
- An individual at an organisation can only access the EHR if the data subject is registered at the organisation as needing care services.
- The ability for the data subject to request that individual items within their EHR remain private and are therefore not shared beyond the caring organisation who recorded the item.
- An individual will not be able to access records flagged as Spine sensitive.
- Data recorded that is within the SCR exclusion set will be hidden when viewing the record.
- New organisations joining SystmOne start in a 'switched off' state in terms of the integration. The integration can be enabled by TPP in the stage of controlled pilot, and will move towards the model where organisations have control over switching the integration on or off themselves.
- A SystmOne user screen that lists all organisations that are sharing outside SystmOne, with 'type' descriptors (e.g. General Practice, Urgent Care, A&E department, etc.), which are configured based on the organisation name or ODS code.
- A screen within SystmOne to allow the care organisations to set up their current default sharing rules.

Appendix B - Summary of Processing Operations

Description	Details
Subject matter of the Processing for the Integrations	The Processing is of health and social care data relating to those patients who are receiving care within the NHS, including providers commissioned and paid by the NHS, by Local Authorities. The care settings using the integration between SystmOne and Third Party systems are currently as follows: • GP practices • Community services such as district nurses, rehabilitation centres, telehealth and diabetes services • Child health services that undertake scheduling of treatments such as vaccinations • Urgent care organisations such as Minor Injuries Units and Out of Hours services • Community hospitals • Palliative care hospices and community services

	• <i>NHS Mental Health trusts</i> • <i>NHS Hospital trusts</i> • <i>Accident and Emergency departments</i> • <i>Care Homes</i> • <i>Social Care – registered and regulated professionals within social care organisations co-ordinating care (not social care providers)</i> <i>Some of these health records will contain highly sensitive information such as medical diagnoses and associated information.</i>
<i>Duration of the Processing</i>	<i>The duration of processing is within the retrieval of the patient record. No data will be retained during this retrieval.</i>
<i>Nature and purposes of Processing</i>	<i>The nature of the processing means any operation such as retrieval, consultation, use, disclosure by transmission whether or not by automated means, etc.</i> <i>The purpose is to allow health professionals, who have the appropriate controls and access rights, to view electronic health records (EHRs), for the medical treatment of individuals (this includes care relating to their mental health and social care provision).</i> <i>The data is stored in England.</i> <i>Details of any sub-processors – N/A</i>
<i>Type of Personal Data</i>	<i>Name, address, date of birth, NHS number, telephone number, email address, ethnicity, religion, gender, medical diagnoses, medications, allergies and sensitivities, medical history.</i>
<i>Categories of Data Subjects</i>	<i>Any individual attending for care services who could include;</i> • <i>Children</i> • <i>Vulnerable adults</i> • <i>Individuals sectioned under the Mental Health Act (MHA)</i> • <i>The elderly</i>
<i>Data Protection Officer</i>	<i>Dr John Parry</i> <i>dpo@tpp-uk.com</i>