Mid and South Essex Sustainability and Transformation Partnership

A programme to sustain services and improve care

Pre-consultation Business Case

Appendix 5 – Privacy Impact Assessment

Privacy Impact Assessment

This annex describes the mid and south Essex STP approach to Information Governance assurance, which is based on NHS England's guidance for new systems documented in "IG Requirements for New Processes, Services, Information Systems and Assets" and the Information Commissioners Office guide for the application of Privacy Impact Assessment" published in November 2015. Initial proposals have been reviewed by the PIA Working Group and there are plans for further reviews for assurance. This section also describes how the STP proposals meet the Caldicott Principles for Information Governance and prospective need for clear deliverables within the Enabler work programme.

Introduction

The mid and south Essex STP has based its approach to the application of the Privacy Impact Analysis (PIA) on NHS England's guidance "IG Requirements for New Processes, Services, Information Systems and Assets" published in March 2014. It also draws on the guidance from the Information Commissioners Office on "Privacy Impact Assessment Code of Practice" published in February 2014. Additionally the requirements of the HSCIC guide "Code of practice on confidential information" which supports the development of good practice for organisations collecting, analysing, publishing or otherwise disseminating confidential information concerning, or connected with, the provision of health services.

The mid and south Essex STP IG Working Group has undertaken the following assurance reviews and processes

- Review by the East of England IG Working Group
- Assessment against the options for service change
- Review and assurance from the IG Oversight Group
- Privacy impact assessment

This section outlines the PIA approach and how the review was carried out. Additional details of mitigation of risk is included to support the Enablers identified in Section 8.

Review by the Information Governance Working Group

In June 2016 a panel of the East of England Information Governance leads was engaged to provide independent advice on the proposals from the STP. The scope of the panel review was to undertake a Privacy Impact Assessment, recognising that, in addition, there were strong interdependencies between reconfiguration and other initiatives in the overall programme, particularly the adoption of new pathways of care which might impact privacy and confidentiality issues.

Key questions for the working group to consider included

- Did the options create additional risk, or reduce risk, for data security and privacy?
- Are there other impacts that should be assessed or other unintended consequences that have not been measured?

The Working Group was supplied with background materials on proposals and process. Supporting information from the Local Digital Roadmaps was also made available to provide context for the options submitted. The Working Group then followed up with any clarification questions necessary to fully understand the proposals being made.

Summary of Working Group recommendations

The Working Group was broadly supportive of the programme. Given the scale of the challenge, they acknowledge this was a real opportunity and possibly the only opportunity for some years, to make a real difference.

The working group recognised that many of the risks and issues encountered in the Options were not new, nor were they specifically associated with the options proposed. However this was an opportunity to implement the “privacy by design” concept and therefore many of the current risks could be addressed during design rather than on an ad-hoc basis once the solution has been implemented.

The panel identified a number of areas where more work was needed, namely more detailed activity and interface modelling, assessment of the Need to Know Principle, and demonstration of links between in hospital and out of hospital work. The full PIA report from the Information Governance working Group is included in this update.

Response to Working Group recommendations

The report from the IG Working Group was circulated to the Review & Oversight Group to aid development of proposals. Each recommendation has been responded to as outlined in Appendix 8 (cross check this j dixon) .

The oversight group discussed the observations and recommendations generated by the Working Group and have agreed the Privacy Impact Assessment

Privacy Impact Assessment

1.1.1. Methodology Approach

PIAs are endorsed by ICO for assessment of IG compliance. The working group was aware of the diverse nature of the organisations involve in the STP, however due to the significant involvement of NHS and Healthcare organisations it was agreed to use the NHS England template rather than the ICO equivalent.

Assessment of Main Plan

Criteria	Impact/Issue
• Increased scope of stakeholders engaged with information	As systems and services integrate the diversity of data will increase and the variety of records and record keeping will grow more complicated. This growth in range and complexity will present a risk to the value of information derived from records. Additionally as services become more remote from Users and professionals the need for up

	to date, accurate and complete records becomes more relevant to service delivery and quality. Options must identify how, in a more integrated environment, the need-to-know principle and the value of information will be protected.
• Further integration of systems, including interfaces	As service integration is implemented, supporting informatics will need to keep pace. This means either integration of supporting applications or the development of further interfaces to ensure data is available to all members of the clinical team. As integration/interfaces develop there is a greater risk of error, failure, or malicious attack. Any local system enhancement must sustain security and privacy within new functionality delivered to support the STP.
• Greater use of electronic data capture	Much of the STP options relie on modernisation of the processes undertaken. This includes a significant demand for data capture at point of care, both within acute care and also in community settings. The delivery of data capture at point of care involves a number of innovations which present risk to personal data. Mobile data capture presents risk of loss, theft or failure which will impact the delivery of service. The collection of data off-line, batch or in real-time each have incumbent risks which will need to be addressed. The operational use of systems which may not be locally developed will increase the need for staff training and support. The need for all staff to be trained and competent in the use of both hardware platforms and software applications will significantly impact the training and development needs of all staff. There is a likelihood that some elements of training will need to move to a virtual classroom with training being delivered in a flexible way electronically. This would allow for self-paced and self-service training to become the norm within the system.
• Increased sharing and exchange of information between clinicians/organisations	The need for more novel pathways of care will require larger teams involved in the care of an individual. This expansion of the care team will necessitate an increase in communication between team members who may not be co-located and will likely be in differing organisations. Since unintended disclosure is the single largest class of SIRI any increase in communication between sites and team members will lead to increases in risk of inappropriate disclosure or disclosure in error. Unless systems are integrated electronically then all forms of correspondence between team members is prone to error and mistake.
• Higher dependency on information and data analytics	Any integrated service infrastructure will require greater dependence on information available across the system. Whether this is management or operations the element of hands-on control and individual awareness will be significantly reduced once the system becomes a single large integrated healthcare economy. The comprehension of system events will not be held by individual local experts, but will rely on process and signposting from information flowing around the system. Information will

	change over time and will also change in context. This means that the dependency on information is increased and universality of analytics will decline proportionately. Adjustments to data in context may reduce the ability for central analytical service providing answers to everyone!
• Greater dependency on robust delivery of a technology platform	The requirement for integrated working from virtual teams across multiple sites and organisations means that the technology platform becomes a priority for the delivery of service. Any restricted operation or failure within the platform will significantly impact the delivery of service. Potential for alternative ways of working, or secondary system operation, must be validated as the change to operations structures is developed. Robust business continuity plans will be required to ensure that system collapse is avoided

Option Assessment

The options for future service delivery identify a common theme for successful delivery which is predicated on a greater use and dependence on technology across the organisations and system. This dependency includes higher risk on system operation (both hardware and software) and the ability of clinical and administrative/managerial staff to deliver efficient and effective healthcare service.

Approach be taken by mid and south Essex

Public and patient engagement has been a foundation of the programme. It has been included in the following ways.

Many local people who take an interest in the STP plan have a keen interest in the issue of shared information and information technology. This subject came up in discussions at most of our engagement events and public workshops. Further details on this and local views on the matter are in annexe 7, which is a summary of feedback during public and patient engagement. On the whole, we noted that public attitudes have changed from where they were a few years ago when NHS organisations were first consulting on shared patient records. At that time, there was some resistance to the possibility and a fear of losing patient confidentiality. During our 2016 engagement programme, most of the views on information were in support of accelerating developments to enable shared information and to make the best use of the information technology available.

2.

3. Data Protection Act 1998

4. PRIVACY IMPACT ASSESSMENT (PIA)

5. Compliance Checklist

6. Privacy

7.

8. Privacy has become a much larger consideration for business and government in recent years. New information technologies have increased public concerns about intrusion into their privacy.

9.

10. Beyond the recognition of privacy as a human right, specific laws have been introduced to deal with particular areas of concern. Much of the legislative attention to date has been focused on information about people that is collected, stored, used and disclosed by organisations. The handling of personal data is regulated by the Data Protection Act 1998, which the Information Commissioner's Office oversees.

11.

11.1. Privacy impact assessment

Privacy Impact Assessment (PIA) is a process which enables organisations to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be managed through the gathering and sharing of information with stakeholders. Systems can be designed to avoid unnecessary privacy intrusion, and features can be built in from the outset that reduces privacy intrusion.

This Privacy Impact Assessment (PIA) aims to assist NHS England when proposing change to investigate whether the personal information aspects of their project comply with the data protection principles in Schedule 1 of the Data Protection Act (DPA).

It should be noted that many terms used in the principles have meanings specific to the Data Protection Act, and it would be prudent to refer to the Act for definition for those terms. Another useful reference is the specific guidance on the Information Commissioner's website (www.ico.gov.uk). General advice is contained in the Commissioner's Legal Guidance.

12.

I BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Lead Directorate and project name	
Directorate	**Mid and South Essex Success Regime**
Department	**Information Governance Working Group**

Project	A programme to sustain services and improve care in Mid & South Essex

2. Contact position and/or name, telephone number and e-mail address. (This should be the name of the individual most qualified to respond to the PIA questions)	
Name	Peter Manser
Title	Information Governance Lead
Phone Number	01138 254 987
E-Mail	Peter.manser@nhs.net

3. Description of the programme / system / technology / legislation (initiative) being assessed.

The PCBC document considers proposed changes to health and social care services in Mid and South Essex. It aims to make the case for commencing public consultation for the Success Regime by setting out:

- The clinical and financial case for change;
- A vision for the future;
- A future model of care for in hospital and out of hospital services;
- System-wide enablers and governance for clinical proposals;
- Options for reconfiguration and redesign of services, and a framework for evaluating their likely impact;
- Engagement to date and consultation plans;
- A high level implementation plan for proposed changes;

4. Purpose / objectives of the initiative (if statutory, provide citation/reference).	
Purpose	The Success Regime aims to address 6 (six) identified challenges which became apparent from the Diagnostic Phase. These are; • A clinically and economically disadvantaged acute footprint • Workforce and talent gaps • A complicated commissioning landscape • Protracted decision-making • Senior managerial / clinical leader capacity focused on operational needs • Limited data usage and data sharing .

5. What are the potential privacy impacts of this proposal?
• Increased scope of stakeholders engaged with information
• Further integration of systems, including interfaces
• Greater use of electronic data capture
• Increased sharing and exchange of information between clinicians/organisations
• Higher dependency on information and data analytics
• Greater dependency on robust delivery of a technology platform

IF THERE IS NO PERSONAL DATA INVOLVED,
GO TO SECTION III DPA COMPLIANCE - CONCLUSIONS (on the last page)

***IMPORTANT NOTE:**
'Personal data' means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

(Data Protection Act, section 1)

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance pages 19-35

1.1 Preliminary	
What type of personal data are you processing?	Personal data
	Clinical/Health Data including psych, Social care data
1.2 Schedule 2 Conditions relevant for purposes of the first principle: processing of any personal data	
Describe the purposes for which you will be processing personal data.	Provision of Health and social care. Management, planning and delivery of health and care services. Research and development of efficient and effective service provision
List which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data.	CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA 1. The data subject has given his consent to the processing 2. The processing is necessary (a)for the performance of a contract to which the data subject is a party, or (b) for the taking of steps at the request of the data subject with a view to entering into a contract. 3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract 4. The processing is necessary in order to protect the vital interests of the data subject 5. The processing is necessary (a)for the administration of justice, (aa)for the exercise of any functions of either House of Parliament, (b)for the exercise of any functions conferred on any person by or under any enactment, (c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or (d)for the exercise of any other functions of a public nature exercised in the public interest by any person. 6. (1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. (2)The Secretary of State may by order specify

	particular circumstances in which this condition is, or is not, to be taken to be satisfied.
1.3 Schedule 3 Conditions relevant for purposes of the first principle: processing of any *sensitive* personal data	
If this project does not involve the processing of sensitive personal data, please go to section 1.4	
Identify the categories of *sensitive personal data* that you will be processing.	• Clinical Health Data • Social Care Data
Identified *the purposes* for which you will be processing *sensitive personal data*.	Medical purposes, including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
Identify which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing *sensitive personal data*?	1. The data subject has given his explicit consent to the processing of the personal data. 2. (1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment. (2)The Secretary of State may by order— (a)exclude the application of sub-paragraph (1) in such cases as may be specified, or (b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied The processing is necessary; (a)in order to protect the vital interests of the data subject or another person, in a case where— (i)consent cannot be given by or on behalf of the data subject, or (ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld. 4. The processing. (a)is carried out in the course of its legitimate activities by anybody or association which— (i)is not established or conducted for profit, and (ii)exists for political, philosophical, religious or trade-union purposes, (b)is carried out with appropriate safeguards for the rights and freedoms of data subjects, (c)relates only to individuals who either are members of the body or association or have regular contact with

	it in connection with its purposes, and (d) does not involve disclosure of the personal data to a third party without the consent of the data subject. 5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject 6. The processing (a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), (b)is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights. 7. (1)The processing is necessary (a)for the administration of justice, (aa)for the exercise of any functions of either House of Parliament, (b)for the exercise of any functions conferred on any person by or under an enactment, or (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
1.4 Obtaining consent	
Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2?	**Yes** ✓ **No**
If yes, when and how will that consent be obtained?	Declaration on registration with the GP practice. NHS Data Choices inc. Type 1 and Type 2 Consent to Share. Informed explicit consent for procedures within secondary care.
For the processing of *sensitive personal data*, are you relying on *explicit* consent as specified in Schedule 3, s1 of the Data Protection Act?	**Yes** ✓ **No**
If yes, when and how will that consent be obtained?	Declaration on registration with the GP practice. NHS Data Choices inc. Type 1 and Type 2 Consent to Share. Informed explicit consent for procedures within secondary care. Other Data Controllers (eg Local Authority) will manage their own local consent models
1.5 Lawful processing	
How is compliance with the Human Rights Act being assessed?	Via this PIA Review and the Data Sharing Agreement - Information is limited to a need to know and informed consent is provided to ensure no breach of Human Rights occurs. NHS

	policy and mandated compliance with NHS Digital IG Toolkit ensures HRA compliance
Are you assessing whether your processing is subject to any other legal or regulatory duties?	**Yes** ✓ **No**
If yes, how is that assessment being made? If no, please indicate why not.	Inclusion of NHS IG Guidance incl. DPA, AHRA etc. Requirements for other agencies inc Police, LA and CSSR will be locally managed within the overall service delivery
1.6 Fair processing	
How are individuals being made aware of how their personal data is being used?	Fair Processing notice on NHS Choices and stakeholder website
How individuals are offered the opportunity to restrict processing for other purposes?	Through direct contact with the stakeholder staff and via GP recording of Opt-Out preferences
When is that opportunity offered?	Patient can communicate with stakeholders or GP during any consultation, or at anytime
1.7 Exemptions from the first data protection principle	
The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller 2. the identify of any nominated data protection representative, where one has been appointed 3. the purpose(s) for which the data are intended to be processed 4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair *Data Protection Act, Schedule 1, Part II, para. 2 (3)*	
Do you provide individuals with all of the information in the box above?	**Yes** ✓ **No**
If no, which exemption to these provisions is being relied upon?	

PRINCIPLE TWO: **THE PURPOSE OR PURPOSES FOR PROCESSING PERSONAL DATA**		
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. *For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance pp 35-6*		Risk Profile Assessment
2.1 Use of personal data within the organisation		
What procedures are in place for maintaining a comprehensive and up-to-date record of use of personal data?	The Options propose a significant increase in joint working, with corresponding devolved data capture throughout the system. Unless specific datasets are provided with a structure of Information Asset Owners then it remains difficult to maintain data quality and the provision of up-to-date records. Since the proposed Options do not provide identification of information governance for the assurance of data quality this remains a significant risk. The Options refer subjectively to real-time data capture at point of care, and distributed interfaces between systems. Without strong update rules the joint management of data across system creates a potential for difficult version control for patient data. The omission of a common coding structure across the various systems will create significant difficulties in the interpretation of code data. This may prohibit data flows from Acute into/between community/GP systems. This lack of a common clinical terminology will limit the usefulness of information exchange between stakeholders	
Is any data processing carried out on your behalf (e.g. by a subcontractor)?	**Yes** ✓ **No**	
If yes, please identify	A number of commissioned subcontractors exist within the Health economy. These include charitable & Voluntary Sector, Commercial and not-for-profit providers in various clinical/welfare areas. The inclusion of these, often small, providers presents a significant threat to the confidential processing of data. Unless adequate governance arrangements can be established and maintained across the sub contract community then this will continue to present a threat to patient data. The growing use of non-NHS providers in both health and social care provision means that greater data flow and the necessary operational processing of data, present potential areas for concern.	

	While larger organisations can afford the necessary infrastructure to deliver privacy and confidentiality, smaller providers may struggle to ensure that all aspects of IG are delivered robustly.		
2.2 Use of existing personal data for new purposes			
Does the project involve the use of existing personal data for new purposes?	**Yes** ✓ **No**		
If no, go to section 2.3	The existing data sets are used and processed within specific silos, this leads to restricted information value being added to the data. The re-use of data between operational areas, both within pathways and between agencies can lead to greater efficiency for services and a higher effectiveness in planning and delivery. While the re-use may have specific benefit to the health economy, the data subject may need to provide additional consent for these changed purposes to be realised. The inclusion of Patient Opt-out may create significant difficulties for operational delivery		
If yes, How is the use of existing personal data for new purposes being communicated to:- a) *the data subject:* b) *the Data Protection Officer (responsible for Notification)*	a)	In directly via public consultation on the Success regime. Specific reference to information governance may be included into the communication and engagement plan surrounding the programme	
	b)	Significant revision of FPN and DPA registration will be required for each stakeholder. Additionally the issue of Data Controller in Common, or Joint Data Controllers will need to be resolved and documented. The could require revision of DSA and ISP across the sector	
2.3 Disclosure of data			
How individuals / data subjects are made aware of disclosures of their personal data?	The significant development of integrated pathways and shared care will require significant disclosure of data. Additionally the joint working between Primary and Secondary care and between Health and Social care will take significant planning and modelling to ensure that the legitimate relationships and appropriate data flows are documents wand defined for FPN et al. This presents a significant risk since this has not been done before and involves a new solution model.		

PRINCIPLE 3: **ADEQUACY AND RELEVANCY**		
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. *For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance pp 36-37*		
3.1 Adequacy and relevance of personal data		
How is the *adequacy* of personal data for each purpose determined?	It is not clear from the options proposed how the definition of "need to know" will be managed within the proposals. Given the novel and potentially unique design of service delivery the requirement for adequate data scoping remains unclear	
How is an assessment made as to the *relevance* (i.e. no more than the minimum required) of personal data for the purpose for which it is collected?	It is not clear from the options proposed how the definition of "need to know" will be managed within the proposals. Given the novel and potentially unique design of service delivery the requirement for adequate data scoping remains unclear	
What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?	Currently none of the options identify an assurance process which would review data scope issues. It is possible that a process of iterative refinement could address these issues, but would only act retrospectively on data sets.	

PRINCIPLE 4: **ACCURATE AND UP TO DATE**			
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance pp 36-37			
4.1 Accuracy of personal data			
How often is personal data being checked for accuracy?	Personal data is reviewed on a routine basis whenever a patient presents within the boundaries of the ESR. The enlarger number of players means that contact with a patient may be more frequent within an integrated solution than would be the case with isolated organisations.		
How is the accuracy of the personal data being checked with the Data Subject?	A number of validation processes are provided incl. Face-to-face and system checking through patient tracing with open Exeter However the integration of data, and the synchronisation of systems is not addressed within the proposed options. The nature of change and the speed of propagation of any change in parts of the system is not addressed. This could create consistency problems and require the patient/service user to repeat details across the system to enable changes to be made.		
4.2 Keeping personal data up to date			
How is personal data evaluated to establish the degree of damage to: (a) the data subject or (b) the data controller that could be caused through being out of date?	a)	Clinical practice within Primary, community and acute providers ensures that records remain timely, complete and accurate. Existing protocols around SAR or AHRA would need to be revised in respect of the richer record management within the integrated environment. Redaction and disclosure may need to be review between partners	
	b)	The options proposed do not directly address the changes to record keeping, and therefore the degree of damage accidental loss or disclosure may have on organisation. The enlarged record and the role of "need to know" would need to be addressed for assessment of risk.	

PRINCIPLE 5 **NO LONGER THAN NECESSARY**		
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. *For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance p 39*		
5.1 Retention policy		
Is the project subject to any statutory / sectorial requirements on retention?	**Yes** ✓ **No**	
If yes please state relevant requirements	○ NHS Records Policy ○ Statutory retention of Health Records	
5.2 Review and deletion of personal data		
When data is no longer necessary for the purposes for which it was collected: a) How is a review made to determine whether the data should be deleted? b) How often is the review conducted? c) Who is responsible for determining the review? d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?	a) Application of NHS Record Retention Guidelines	
	b) Application of NHS Record Retention Guidelines	
	c) Self-assessment by organisations	
	d) Unknown at this time	
If yes, please explain		
Are there any exceptional circumstances for retaining certain data for longer than the normal period?	**Yes** ✓ **No**	
If yes, please provide justification	Certain Forensic Psychiatric records	
PRINCIPLE 6 **SUBJECTS RIGHTS/SUBJECT ACCESS**		
Personal data shall be processed in accordance with the rights of data subjects under this Act. *For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance pp 39-40*		
6.1 Subject access		
How do you locate all personal	The responsibilities, in particular Data Controllership has not been defined or	

data relevant to a request (including any appropriate 'accessible' records)?	documented. The integrated delivery proposed within the options would potentially lead to Controllers in Common. It is therefore unclear how individual data subjects would access date. Although the primary key for all records would be NHS Number, the interpretation of coded data across the system may be difficult.	
6.2 Withholding of personal data in response to a subject access request		
Are there any circumstances where you would withhold personal data from a subject access request?	**Yes** ✓ **No**	
If yes, on what ground. If no, go to 6.3	Damage or Distress to patient/Data Subject – third party data	
How are the grounds for doing so identified?	Review by responsible clinician	
If yes, please provide justification	As per guidelines	
6.3 Processing that may cause damage or distress		
Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?	**Yes** ✓ **No**	
If yes, please specify proposed procedures. If no, please indicate why not.	Via clinical engagement and counselling	
Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?	**Yes** ✓ **No**	
If yes, please explain	Liability and Professional indemnity insurance	
6.4 Right to object		
Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?	**Yes** ✓ **No** **N/A** **Other**	
If yes, please explain	Specific READ Codes for suppression of data extraction – it is unclear how this opt-out would be managed through secondary acute care, or via LG Social care records	
6.5 Automated decision		
Are any decisions affecting individuals made solely on processing by automatic	**Yes** ✓ **No**	

means?		
If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?	Generally risk stratification and screening in via auto select process. This is made clear in any associated correspondence	
6.6 Rectification, blocking, erasure and destruction		
What is the procedure for responding to data subject's notice (in respect of accessible records) or a court order requiring: a) rectification; b) blocking; c) erasure or; d) Destruction of personal data?	a) General struck through and annotate.	
	b) Possible from selective update	
	c) Not usually possible	
	d) In line with NHS Records Management policy	

PRINCIPLE 7 **SECURITY OF PERSONAL DATA**		
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. *For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance pp 40-3*		
7.1 Security Policy		
Is the level of security appropriate for the type of personal data processed?	**Yes** | | **No** | ✓	
If yes please explain	In development and implementation of any option the necessary security policy would need to be developed in parallel. This would need to identify both storage and transmission of data within the preferred solution.	
7.2 Unauthorised or unlawful processing of data		
Describe security measures that are in place to prevent any unauthorised or unlawful processing of: a) Data held in an automated format e.g. password controlled access to PCs b) Data held in a manual record e.g. locked filing cabinets	a) Initial system protected by User Id and Password. National systems further protected by Chip and Pin smart cards	
	b) All paper records and notes protected via locked cabinets. Building security and access codes.	
Is there a higher degree of security to protect *sensitive personal data* from unauthorised or unlawful processing?	**Yes** | ✓ | **No** |	
If yes, please describe the planned procedures. If no, please indicate why not.	RA management of Smart Codes to staff	
Describe the procedures in place to detect breaches of security (remote, physical or logical)? **logical (such as hacking etc.)*	Individual systems may have audit log of access request and refusal. Methods depend of application system selected within each solution and associated compliance with IG Toolkit. During implementation systems may require further protection of data to prevent drift to lowest common denominator	
7.4 Destruction of personal data		
Describe the procedures in place to ensure the destruction of personal data	Based on self-assessment of compliant with NHS Record Management Policy and guidelines	

no longer necessary?					
7.5 Contingency planning					
Is there a contingency plan to manage the effect(s) of an unforeseen event?	**Yes**	✓	**No**		
If yes, please give details	Standard EPRR management within individual organisations. IT systems using routine disaster recovery measures (data back-up and alt site use)				
Describe the risk management procedures to recover data (both automated and manual) which may be damaged/lost through: a) human error b) computer virus c) network failure d) theft e) fire f) flood g) other disaster.	a)	Unspecified local organisational methods			
	b)	Unspecified local organisational methods			
	c)	Unspecified local organisational methods			
	d)	Unspecified local organisational methods			
	e)	Unspecified local organisational methods			
	f)	Unspecified local organisational methods			
	g)	Unspecified local organisational methods			
7.6 Choosing a data processor					
How do you ensure that the Data Processor complies with these measures?	Ensure that Tender complies with required policy and procedure				

PRINCIPLE 8 **OVERSEAS TRANSFER (OUTSIDE OF THE EEA)**				
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. *For the Information Commissioner's general guidance in relation to this DPP, see Legal Guidance pp 43-5*				
8.1 Adequate levels of protection				
Are you transferring personal data to a country or territory outside of the EEA[1]? [1] The European Economic Area (EEA) comprises the 27 EU member states plus Iceland, Liechtenstein and Norway.	**Yes**		**No**	✓
If no, go to Part III If yes, where?				
What types of data are transferred? (e.g. contact details, employee records)				
Are *sensitive personal data* transferred abroad?	**Yes**		**No**	
If yes, please give details				
Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?	**Yes**		**No**	
If yes, please describe. If no, please indicate why not.				
Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?	**Yes**		**No**	
If yes, please give details				

III DPP COMPLIANCE - CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

The absence of detailed design and documentation prevents the identification of specific service data sets, or the application of a need-to-know principle to the integrated, technologically assisted, model of care described in the Success regime proposals. This absence of detail requires that the Privacy Impact Assessment records:

LIMITED ASSURANCE of the proposal as documented at this stage.

IG Manager/DPO Name – Peter Manser

IG Manager/DPO Signature

Date - DD MMM YYYY

Chair ESR PIA Oversight Group – **TBA**

Signature-

Date - DD MMM YYYY