Data Protection Impact Assessment (DPIA)

Project Title:	**Electronic Palliative Care Co-ordination System (ePaCCS) in Humber, Coast and Vale**	
Project Description:	As part of the Local Health and Care Record Exemplar (LHCRE) programme, EPaCCS is to be deployed across Humber, Coast and Vale. EPaCCS enables the recording and sharing of a patient's care preferences and key details about their care at the end-of-life and will eventually form part of the wider LHCRE programme. As it is electronic it can easily be shared 24/7 between all of the clinicians and carers involved in the patient's care across organisational and geographical boundaries.	
Project Manager Details:	Name:	
	Title:	Business Change Lead
	STP:	Humber, Coast and Vale
	Telephone:	
	Email:	
Implementation date:	October 2019	

Information Asset Owner (IAO): (All systems/assets must have an Information Asset Owner (IAO).	Name:	John Mitchell
	Title:	Associate Director of IT
	STP:	Humber CCGs
	Telephone:	
	Email:	

Information Asset Owner (IAO): (All systems/assets must have an Information Asset Owner (IAO).	Name:	Debbie Westmoreland
	Title:	Head of Digital
	STP:	NHS Scarborough & Ryedale CCG
	Telephone:	
	Email:	

Information Asset Administrator (IAA): (All systems / assets must have an Information Asset Administrator (IAA) who reports to the IAO as stated above. IAA's are normally System Managers / Project Leads)	Name:	Tara Athanasiou
	Title:	Business Change Lead
	STP:	Humber, Coast and Vale
	Telephone:	
	Email:	

Information Governance Approval
Head of Information Governance and Complaints (Data Protection Officer), North East Lincolnshire Council and CCG
Information and Data Protection Manager, Hull City Council and CCG
North Lincolnshire CCG
East Riding of Yorkshire CCG
Vale of York CCG
Scarborough & Ryedale CCG

Data Protection impact assessment screening questions:

Answering 'yes' to any of these questions is an indication that a DPIA is a necessary exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions if necessary for unusual circumstances.

Questions	Yes/No
Will the project involve the collection of new information about individuals?	no
Will the project compel individuals to provide information about themselves?	no
Will information about individuals be disclosed to 3rd party organisations or people who have not previously had routine access to the information?	yes
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	no
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	no
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	no
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	yes
Will the project require you to contact individuals in ways which they may find intrusive?	no

Step One: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

Patients who are at the end of life come into contact with many health and care professionals. The challenge has been in enabling different care providers to share information about an individual patient's care and end-of-life preferences in a safe, up-to-date and efficient way.

Treatment choices, how and where care is delivered and the preferred place of death are at the heart of end-of-life care. Patient choices are not static and often change during the last weeks and months of life. Typically, preferences for end-of-life care are collected by GPs and inputted into their GP system. However, this may not always reflect the latest wishes of the patient and may not be available to all of a patient's health and care providers.

The emphasis being placed on improving end-of-life care is also reflected within the contractual standards being implemented for health and care providers, for example with two new QOF indicators introduced in the new GP contract that focus on quality improvement and shared learning. EPaCCS can support health and social care providers in meeting end-of-life contractual standards as part of the improvement of the full end-of-life care management process.

What is EPaCCS?

EPaCCS (Electronic Palliative Care Co-ordination System) enables the recording and sharing of a patient's care preferences and key details about their care at the end-of-life. As it is electronic it can easily be shared 24/7 between all of the clinicians and carers involved in the patient's care across organisational and geographical boundaries.

An EPaCCS record can be created, updated and shared by any member of a patient's health and care team, subject to locally-determined pathway and user administration settings. The EPaCCS record is a summary record, intended to provide an easily accessible view of the information that carers need in an end-of-life setting. Some of the data that populates the EPaCCS record is pre-populated from the GP record, for example, patient demographics, GP practice details, current repeat medications and diagnoses/problems. Other mandatory fields can be filled collaboratively by different health and care providers, including:

- Primary end of care diagnosis
- CPR decision
- Preferred place of care
- Details on anticipatory medication
- Preferred place of death.

How have clinicians been involved in EPaCCS?

We have chosen to work with Black Pear to deliver the EPaCCS solution. Black Pear has worked collaboratively with GPs, Macmillan GPs, Hospice Palliative Care Consultants and Community

Palliative Care Consultants to develop a clinically-focused EPaCCS form.

After an initial clinical workshop, we have convened a Clinical Design Authority with representatives across the health and care providers involved in end-of-life care. This Clinical Design Authority is responsible for ensuring that the EPaCCS solution meets our local priorities and pathways and will make any local changes required to the forms. After the pilot, a full clinical review will take place, at which point any further changes will be made before the full roll-out of the solution across Humber Coast and Vale.

Why the need for a DPIA was identified

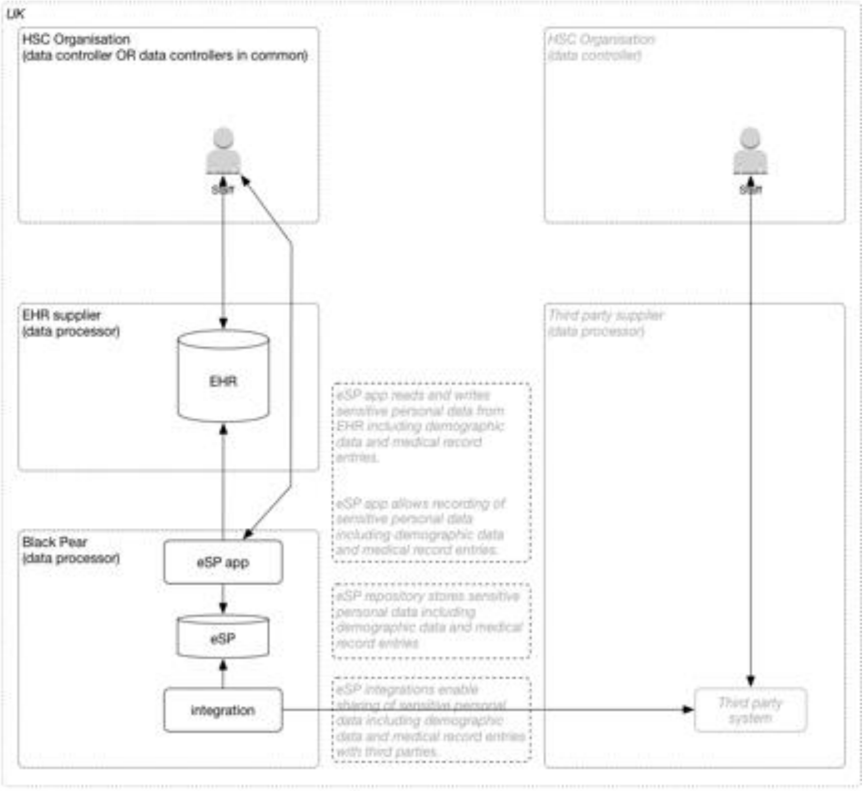
The need for a DPIA was identified because EPaCCS involves the electronic sharing of information about patients' end of life care and preferences and the requirement to ensure that this information is shared appropriately, securely and with respect to the patient's wishes and rights to privacy. EPaCCS is intended to address the challenge currently faced, where some carers or clinicians may not be aware of a patient's latest preferences because of no standardised ways of sharing end-of-life information. This information is currently shared between carers and clinicians in a variety of formats (for example, by paper-based care plan, phone or entered directly into the OOH system by GPs in some instances) but information about a patient's preferences is not routinely available. The EPaCCS will enable the sharing and updating of a patient's end of life preferences and care between all clinicians and carers directly responsible for their care.

Step Two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

The Black Pear eSP product which has been selected as the EPaCCS solution is used by Health & Social Care Organisations to record sensitive personal data about data subjects including demographic data, medical history and care preferences.

Data Flow


UK
HSC Organisation
(data controller OR data controllers in common)
staff
EHR supplier
(data processor)
EHR
Black Pear
(data processor)
eSP app
eSP
integration
HSC Organisation
(data controller)
staff
Third party supplier
(data processor)
eSP app reads and writes sensitive personal data from EHR including demographic data and medical record entries.
eSP app allows recording of sensitive personal data including demographic data and medical record entries.
eSP repository stores sensitive personal data including demographic data and medical record entries
eSP integrations enable sharing of sensitive personal data including demographic data and medical record entries with third parties.
Third party system

Data Controls

Black Pear processes eSP data within the UK only.

All contracts under which the eSP service operates have been reviewed to ensure that obligations under GDPR are met. Where necessary, clients will be moved to an updated contract by 31st March 2019.

The eSP service is designed to be secure and robust, meeting NHS guidelines and best practices.

Authentication, Authorisation and Security

Authentication

eSP uses Black Pear's BP Auth service (https://auth.blackpear.com) to authenticate users.

Users are authenticated using a unique user identity (their email address) in conjunction with a password.

Credentials cannot be used for authentication until the user has verified their identity and set a strong password. Password strength is checked using Dropbox's zxcvbn library and only passwords that are estimated to take more than 10^10 attempts to guess are allowed.

Passwords will expire after 90 days and a new password must be chosen; this cannot be one of the previous 12 passwords used. If users forget their password then they can simply and easily request a reset link to be sent by email; this allows them to choose a new password:

Apps running in Black Pear's Pyrusium browser synchronise credentials with the linked clinical system so that users are automatically logged into the app, provided that they have logged into the clinical system. For security reasons, BP Auth credentials will need to be re-entered every 14 days.

Passwords are salted and hashed using an NHS approved algorithm before being stored in a secure database managed by Black Pear.

Authorisation
eSP authorises users by using Black Pear's Warden service (https://warden.blackpear.com) to provide robust, token-based authorisation.

Service administrators can assign a role to each user within each eSP service. Users may have different roles on different eSP services.

Role based access control (RBAC) is used to control users' access to system functions within the app and data within services. Users cannot access any system functions or data without having first authenticated and selected their role.

Acceptable Use

The solution will only be used for authorised purposes in accordance with established usage policies of participating direct health and care organisations.

Access Control Management

A designated System Administrator will be confirmed for each of the participating health and care organisation who will have operational responsibility for EPaCCS. The name/s of these individuals must be emailed to: hnf-tr.yhcrhcv.carerecord@nhs.net prior to the set-up of users and the commencement of data sharing.

The System Administrator will determine who will be granted access to EPaCCS within their organisation and the level of access required. The following access levels have been defined:

1. **Create, read and write**
- Any health or care provider who is responsible for the delivery of direct care to a patient

2. **Read and write**
- Any health or care provider who is responsible for the delivery of direct care to a patient
- An administrator who works for a health or care organisation who is responsible for inputting data at the request of a health or care professional who is delivering direct care to a patient. Information can only be added by this user at the direct request of the individual responsible for delivering direct care

3. **Read only**

- Any health or care provider who is responsible for the delivery of direct care to a patient who only needs to view end-of-life information
- Care coordinators who work for health or care organisations (for example, ambulance dispatch centres, Out-of-Hour service co-ordinators)

Each System Administrator will email details of any new users and their required access levels to Black Pear Support, who will create their user accounts.

Each organisation is responsible for ensuring that users are granted the appropriate access to EPaCCS, that they understand the data protection and confidentiality obligations, that all users understand that usage is audited and any mis-use will be reported.

Security

eSP plans are stored in a service-specific Mongo DB replica-set located in a Virtual Private Cloud provided by Amazon Web Services in the EU (London) Region. The private cloud is connected to Transition Network by Redcentric in accordance with an approved Logical Connection Architecture. Redcentric are an NHS Digital N3 aggregator with IGSoC. Black Pear's processes satisfy the requirements of the DSP Toolkit. All data are encrypted at rest using disk-level encryption with approved cryptographic algorithms (AES-256) and only authenticated access is permitted. Data are encrypted in transit using TLS with approved cryptographic algorithms (AES-256). Data are backed up to a geographically separate location at least every 24 hours.

Audit logs record all access to the eSP services and, in addition, local audit logs record all use of the eSP app within Pyrusium. Audit logs are retained for the duration of the service contract and returned to the data controller at the end of the contract.

Standards

eSP authentication, authorisation and security combines industry best practices with relevant NHS requirements including:

- IG Requirements for GP Systems V4
- Password Policy for Non-Spine Connected Applications GPG
- Approved Cryptographic Algorithms GPG

Source code for service authorisation using JWT and HL7 FHIR is published online at:

https://github.com/BlackPearSw/jwt-claims-fhir/blob/master/jwt-claims-fhir.md

Infrastructure scalability, resilience and disaster recovery

Infrastructure
Hosting
Black Pear apps are hosted as a Microsoft Azure Web App. Black Pear services are hosted on Amazon Web Services (AWS) using a Virtual Private Cloud (VPC) in the EU (London) region [eu-west-2].

Network
Connection to NHS networks is provided by Redcentric, an NHS Digital approved N3 aggregator, using an approved Logical Connection Architecture. Redcentric use AWS Direct Connect to provide a physical connection between NHS networks and the VPC.

Third parties
Some services used for additional eSP modules are dependent on APIs provided by Black Pear partners: NHS Digital, EMIS Health, TPP, Vision Health and Docman.

Resilience
Web Apps are available from multiple data centres across Europe to ensure continuity of service in the event of failure in one data centre.

Services are hosted in multiple AWS availability zones in the EU (London) region. For each service, a minimum of N+1 instances are deployed in conjunction with a load balancer in active-active configuration to ensure continuity of service in the event of failure of an instance. Instances are deployed across multiple availability zones (think of an availability zone as a data centre) to ensure continuity of service in the event of a failure in one availability zone. It is not possible to provide continuity in the event of failure of the entire region as this would require the services to process data outside the UK.

Automated health checks are used to detect and replace failed instances; autoscaling is used to detect services reaching capacity limits and to add extra instances to provide additional capacity.

Two network connections are deployed at different physical locations. These operate in an active-passive configuration to ensure continuity of service in the event of failure at one location.

Recovery
All hosted services are routinely deployed using CloudFormation templates to provide fast and repeatable deployments.

Data Retention

eSP data are retained in accordance with [NHS Records Management Code of Practice for Health and Social Care 2016](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016)

Consultation Requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process.

The EPaCCS roll-out in Humber, Coast and Vale is a clinically-driven programme.
A Clinical Design Authority with representatives from across the health and care providers involved in end-of-life care in the region has been convened to ensure that the EPaCCS solution meets the clinical, privacy and personal requirements of patients at the end of life. At the outset of the project, the Yorkshire & Humber LHCRE Information Governance team were engaged to ensure that the IG model used for EPaCCS was designed to address potential privacy risks. This DPIA has been developed with the Data Protection Officer's for North East Lincolnshire and Hull CCGs and will be approved by the SIRO or Caldicott Guardian for each of the six CCGs in Humber, Coast and Vale.

Throughout the pilot process and subsequent full roll-out, privacy risks with be monitored.

The EPaCCS solution uses the Black Pear eSP solution, which has successfully been used in a number of NHS health and care systems to provide an electronic palliative care solution, including the SiDER project in Somerset and Castle Register project in Coventry and Warwickshire.

Step Three: identify the privacy and related risks

Definition of personal data:

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.

Definition of special categories of personal data:

Personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) their political opinions,
(c) their religious beliefs or other beliefs of a similar nature,
(d) whether they are a member of a trade union,
(e) their physical or mental health or condition,
(f) their sexual life and orientation,
(g) genetic data,
(h) Biometric data which can be used to identify an individual,
(i) the commission or alleged commission by them of any offence, or,
(j) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings,

Identify the key privacy risks and the associated compliance and corporate risks. Larger scale DPIA's might record this information on the Trusts formal risk register.

The 7 Data Protection Principles:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, the organisation must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Privacy issue	Comments
Have you identified the purpose of the project?	Yes

Is there a lawful reason you can carry out this project?	Yes - Direct care purposes
How will you tell individuals about the use of their personal data?	Through discussion between the patient and the clinician/carer who initiates an EPaCCS form. An EPaCCS form cannot be completed unless the patient has been informed. Before an EPaCCS can be created for a patient there is a mandatory field that must be completed by the health or care professional that states that the patient has been informed that an EPaCCS is being created for them and that they understand other end-of-life health and care providers will be able to view and amend this information. Each participating organisation will make Privacy Information relating to EPaCCS available according to their policies.
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	N/A
Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act? If yes, is it necessary and proportionate?	No

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the organisation must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Privacy issue	Comments
Does your project plan cover all of the purposes for processing personal data?	Yes
Which personal data could you not use, without compromising the needs of the project?	All information accessible through EPaCCS is necessary for the purpose of end-of-life care.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the organisation must not store any Personal Data beyond what is strictly required.

Privacy issue	Comments
Is the quality of the information good enough for the purposes it is used?	Yes
Which personal data could you not use, without compromising the needs of the project?	Only information that is strictly relevant to the delivery of end-of-life care will be shared. This includes the morbidities of a patient, their medications and their preferences for end-of-life care.

Principle 4: Accuracy

Personal Data shall be accurate and, where necessary, kept up to date. This means the organisation must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Privacy issue	Comments
If you are procuring new software does it allow you to amend and / or delete data when necessary?	Yes.
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Each health and care provider is responsible for the quality and accuracy of data in the system. If errors are identified the errors will be corrected on the system and this will be communicated to the party with inaccurate data.

Principle 5: Storage Limitation

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 is processed. This means the organisation must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Privacy issue	Comments
What retention periods are suitable for the personal data you will be processing? How long will you keep the data for?	We will follow standard NHS data retention procedures.
Are you procuring software that will allow you to delete information in line with your retention periods?	Yes.

Principle 6: Integrity & Confidentiality

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. The organisation must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Privacy issue	Comments
Do any new systems provide protection against the security risks you have identified?	The EPaCCS solution has been procured via GPSoC from Black Pear which is an accredited GPSoC provider.
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	Users of the EPaCCS solution will undergo thorough training on the use of EPaCCS in Humber, Coast and Vale, which will cover technical, local clinical pathway and information governance.
What training on data protection and / or information sharing has been undertaken by relevant staff?	All staff will undertake standard NHS Digital Information Security training or equivalent. All staff MUST be appropriately trained as per the Data Security & Protection Toolkit.
What process is in place to answer 'Subject Access Requests' (requests for personal data)?	The organisation the request is made to will respond in line with their procedures. Where it impacts on other data controllers, reasonable efforts will be made prior to disclosure. Where necessary data subjects will be signposted to the appropriate organisation.
Will the project require you to transfer data outside of the EEA? If yes how does it demonstrate an adequate level of protection?	No
If you will be making transfers outside of the EEA, how will you ensure that the data is transferred securely?	N/A

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance with the data protection principles. This means the organisation must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Privacy issue	Comments
Are Data Protection contracts / Information Sharing Agreements in place with all 3rd parties who will be acting as Data Processors?	Yes
Has the Project been approved / signed off by Information Governance?	Yes – each CCG in Humber, Coast and Vale will approve the Information Sharing Agreement and this DPIA.

Step Four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
The risk of non-functionality of the Black Pear EPaCCS due to a number of different factors (environmental failures, severe network failure, technical component failure, issues within the application, support failings, backup/restore issues, Cyber attack), resulting in potential patient harm and the delay of treatment. The inability to view EPaCCS forms from Black Pear and Regional health and care organisations will also be affected by any outage.	Environmental: All equipment is located in suitable locations with physical security, fire and environmental controls Technical - Server Hardware: Server equipment is covered by suitable hardware maintenance contract, with automated hardware failure alerting Technical: Network level perimeter controls in place for both inbound and outbound access. Technical: Managed a. There are scheduled backups appropriate for the solution; this is daily for most systems. b. Documentation for the solution includes i. Server(s) configuration details ii. Backup process details iii. 3rd party supplier details and responsibilities are defined c. A copy of the backups are stored in a different location away from IT system.	Reduced Reduced Reduced Reduced	

	d. Failed backups are and logged and alerted on e. A business continuity and disaster recovery plan is in place for the Black Pear EPaCCS solution which has been approved by NHS Digital as part of GPSoC Lot 1 and the new GP Futures.		
	Technical - System: standard anti-virus and regular patch management in place. Admin rights controlled, log management in place, and automated monitoring active.	Reduced	
	Technical: Main application and backups are located in multiple Server rooms	Reduced	
	Application: Data is held in the data warehouse	Reduced	
	Application: Most data is held in source systems and available to view	Accepted	
	Backup/Restore: A suitable system and record level backup schedule is in place and proactively monitored for failures. Backups are periodically checked for restorability, and record level restore capability is regularly checked.	Accepted	
	RBAC model used.	Accepted	
	Information Sharing Agreements for partner organisations	Reduced	

Step Five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By
Patient level data exposure to unauthorised individuals.	Information Sharing Agreements and Data Protection contracts for partner organisations and RBAC model used. Secure log-on	The Information Governance leads for each of the 6 CCGs in Humber, Coast and Vale.

Step Six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Ensure Privacy Notice reflects the EPaCCS processing and a suitable Privacy Notice is published by all participating health and care organisations. Incorporate within user and organisational training.	Within one week of approval of the EPaCCS DPIA and ISA	Business Change Lead, Humber Coast and Vale

Contact point for future privacy concerns
The initial point of contact for any privacy concerns is: hnf-tr.yhcrhcv.carerecord@nhs.net. This will be escalated as necessary to the Information Governance lead of the respective CCG.

For further information or guidance, see the ICO's website at http://www.ico.gov.uk

Appendix 1: Data Protection Impact Assessment – Guidance

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously (de-identification).
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely de-identified.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary

Corporate Risks

- Non-compliance with the Data Protection Act 2018; (GDPR) or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Reducing the risks

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.

- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely de-identify the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Organisations will need to assess the costs and benefits of possible privacy solutions. Some costs will be financial, for example an organisation might need to purchase additional software to give greater control over data access and retention. The costs can be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.

Appendix 2 Data Mapping Data Mapping – Guidance

As part of the DPIA process you should describe how information is collected, stored, used and deleted. You should explain what information is used, what it is used for and who will have access to it.

A thorough assessment of privacy risks is only possible if an organisation fully understands how information is being used in a project. An incomplete understanding of how information is used can be a significant privacy risk – for example; data might be used for unfair purposes, or disclosed inappropriately.

This part of the DPIA process can be integrated with any similar exercises which would already be done for example; conducting information audits, develop information maps, and make use of information asset registers.

A Data Flow Map is a graphical representation of the data flow. This should include:

- Incoming and outgoing data
- Organisations and/or people sending/receiving information
- Storage for the 'Data at Rest' i.e. system, filing cabinet
- Methods of transfer

If such data has already been captured covering the proposed project or similar document this can be useful for understanding how personal data might be used.

The information flows can be recorded as a flowchart, an information asset register, or a project design brief which can then be used as an important part of the final DPIA report.

Describing information flows

- Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.
- This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing)
- People who will be using the information are consulted on the practical implications.
- Potential future uses of information are identified, even if they are not immediately necessary.