



Data Protection Impact Assessment Questionnaire

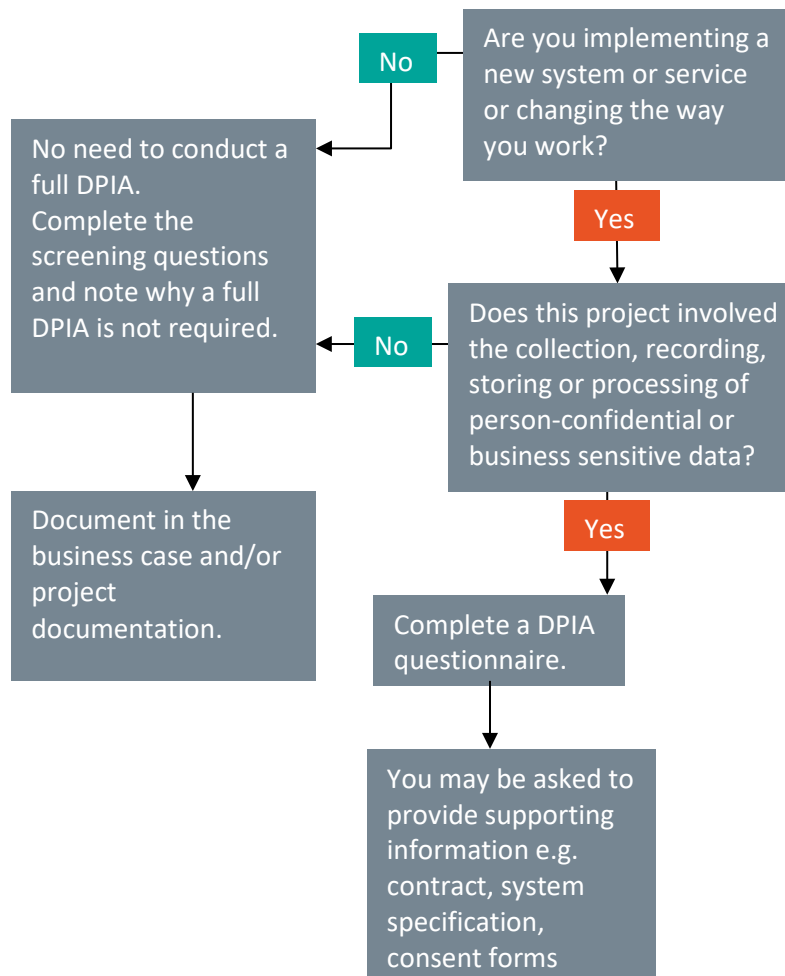
Questionnaire Document revision history

Date	Version	Revision	Comment	Author / Editor
18 July 2018	4	Final		Information Governance Team
24 August 2018	4.1	Final	Replacing current NEL version to align with NHS England version	Information Governance Team
15 January 2019	4.1	Final	Incorporation of comments from consultation with IG Team	Information Governance Team

Questionnaire Document approval

Date	Version	Revision	Role of approver	Approver
26/04/2017	4	Final	Head of IG	[REDACTED]
22/01/2019	5	Final	Head of IG	[REDACTED]
20/03/2019	5	Final	Information Governance Group	Information Governance Group

Do I Need to Complete a DPIA questionnaire?



When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision. Further guidance can be sought from the Information Governance Team: nelcsu.Information-Governance@nhs.net.

It is a requirement of the General Data Protection Regulations that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

If you are assessing a system and it does not have a DPIA, including one that identifies that a full DPIA is not required, please complete the relevant section of this questionnaire.

The questionnaire will be reviewed by the stakeholders, including the IG Lead and the recommendation from the questionnaire will be notified to the Director (Information Asset Owner). The recommendation will be either:

1. A full DPIA is required where the new process or change of use of PCD requires more thorough investigation.
2. The DPIA questionnaire will be signed off by the Information Asset Owner/SIRO and the DPIA log updated by the IG Lead.

There is an Information Security Procurement Questionnaire (for use in the commissioning process for new information systems) available via the IG Team and on SUSI, an Information Risk Questionnaire template and an ICT System Security Risk Assessment available to assist in assessing the risks (embedded in this questionnaire).

1. Project/service stakeholder information

Project/Service Lead contact details	
Your name and base	██████████ Francis Crick House, Northampton.
Your role	Digital Lead, NHS Northamptonshire Clinical Commissioning Group
Your email address and contact number	████████████████████
Information Asset Owner (if different from above)	N/A

Purpose of the Project/Service	
Project/Service Name	Northamptonshire Care Record
In brief, what is the purpose of the project/service and how is the processing of information necessary to that work? Please include expected outcomes.	<p>The historical lack of safe, systematic and planned information sharing across Northamptonshire has been highlighted by the CQC review of Northamptonshire Health and Care Partnership organisations in 2018. The development of the Northamptonshire Care Record will enable sharing of information for the purpose of Direct Care using the CareCentric platform. This Graphnet solution, contracted through Northamptonshire CCG on behalf of the Northamptonshire Health and Care Partnership, provides a robust and secure means to create a consolidated care record, visible across health and care organisations.</p> <p>The Northamptonshire Care Record (NCR) will create a safe and secure environment to share information between organisations involved in providing care to patients and service users within Northamptonshire. This creates a platform to bring together information held on separate systems across Northamptonshire, which is more reflective of current and planned patient and service user pathways.</p> <p>The NCR can be viewed in real time and at the point of care, thereby making it quicker and easier to provide care. This will create a more efficient and effective care system for Northamptonshire, with improved levels of clinical safety and care delivery through reduced duplication and improved</p>

	<p>availability of appropriate care information.</p> <p>The information shared within the NCR, such as investigation results, tests, correspondence and shared care plans will result in fewer duplicated tests, greater transparency and visibility of individual care provision across organisational boundaries.</p> <p>The result will improve the holistic care provision through appropriate visibility of information in all aspects of care. Currently, information held in separate systems such as social services is not visible to health care providers, and health care provider information is not visible to social care providers. This leads to delays within organisations and across pathways, negatively impacting on the timeliness of care received, and ultimately impacting on the service user.</p> <p>The NCR will provide the means of securely sharing appropriate data including care plans, which will improve the quality of life for citizens across Northamptonshire. For example, End of Life care plans will be visible to East Midlands Ambulance Service to ensure that an individual's wishes will be visible to all organisations involved in the care of that individual.</p>
--	--

Timeframe for the Project/Service

When is the Project/Service due to begin? If it's time limited, please note the expected end/review date.	The NCR mobilisation and implementation is already underway. The first set of data from the spine will be uploaded during June 2020 and local providers will begin sharing information in line with the agreed project plan. Once the NCR is fully operational, hosting, maintenance & patching will be the responsibility of Graphnet. Local provider service desks will have responsibility for managing individual service user accounts. The Executive Data Committee (EDC) will have responsibility for governing access and use of the NCR on behalf of Northamptonshire Health and Care Partnership organisations once live, with input from the Northants Data Governance Forum (NDGF).
---	---

Nature of the information

Will all of the information be truly anonymised information ¹ ? Anonymised data must meet the ICO code of practice .	Yes	<input type="checkbox"/>	No – some of the information will relate to an identified or an identifiable person (either directly or indirectly)	<input checked="" type="checkbox"/>
--	-----	--------------------------	---	-------------------------------------

¹ anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

Will the information be new information as opposed to using existing information in different ways?

The information being provided from source systems is not new. It will have the ability to create a care plan held within the CareCentric

Key Contacts

Key Stakeholder Names & Roles:

[REDACTED], IG SME NEL CSU
[REDACTED], DPO and Head of Clinical System Northamptonshire Healthcare Foundation Trust
[REDACTED], Head of Data Quality, Security and Protection Northampton General Hospital NHS Trust
[REDACTED], DPO and Head of Information Governance Kettering General Hospital Foundation NHS Trust
[REDACTED] Information Manager NHS Northamptonshire Clinical Commissioning Group
[REDACTED], Interim DPO Northamptonshire County Council

Date:

27th July 2020

Screening Questions

YES or NO

Will the project involve the collection of information about individuals?

Yes

Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?

No

Will the project compel individuals to provide information about themselves?

No

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes

Are you using **personal data/special category data** about individuals for a new purpose or in a new way that is different from any existing use?

Yes

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make an automated decision about care.

No

Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services

Yes

Will the project result in you making decisions about individuals in ways which may have a significant impact on identifiable individuals? i.e. does the project change the delivery of direct care.

Yes

N.B. If the project is using anonymised/pseudonymised data **only**, the response to this question is "No".

Screening Questions	YES or NO
Will the project require you to contact individuals in ways which they may find intrusive?	No
Does the project involve multiple organisations, whether they are public sector agencies accessing personal data/special category data i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
Does the project involve new or significantly changed handling of a considerable amount of personal data/special category data about each individual?	Yes
Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources?	Yes

If any of the screening questions have been answered “YES”, then please continue with the full Data Protection Impact Assessment Questionnaire (below).

If all questions are “NO”, please return the document to the Information Governance Team and do not complete the full Data Protection Impact Assessment.

Please email the completed screening to nelcsu.Information-Governance@nhs.net

2. Controller/s² and Processors³

Are multiple organisations involved in processing the data? If yes, list below and clearly identify where there is a lead Commissioner or Controller.		Yes/No
		Yes
Name of Organisation	Controller or Processor?	Completed and compliant with the DSP Toolkit ⁴
		Yes/No
Kettering General Hospital NHS Foundation Trust	Controller	Yes
Northampton General Hospital NHS Trust	Controller	Yes
Northamptonshire Healthcare Foundation Trust	Controller	Yes
Northamptonshire CCG	Lead Commissioner and Controller	Yes
Northamptonshire CCG GP Practices (see Appendix A)	Controller	Yes
Northamptonshire County Council	Controller	Yes
East Midlands Ambulance Service NHS Trust	Controller	Yes
Graphnet	Processor	Yes

Has a data flow mapping exercise been undertaken?	Yes/No
If yes, please provide a copy, if no, please ensure this is completed – speak to the IG Team for guidance	Yes

Is Mandatory Staff Training in place for the following?	Yes/No	Dates
• Data Collection:	Yes	On appointment
• Use of the System or Service:	Yes	
• Collecting Consent:	N/A	
• Information Governance:	Yes	Annual

² 'Controller' means alone or jointly with others, the organisation that determines the purposes and means of the processing of personal data – for example, this is the case where an organisation is obliged by law to carry out a specific function

³ 'Processor' means alone or jointly with others, the organisation is processing personal data under the instruction of a Controller and **does not** determine the purposes and means of the processing of personal data – for example, NEL is always a Processor

⁴ The [Data Security and Protection Toolkit](#) is a self-assessment tool provided by NHS Digital to assess compliance to the 10 National Data Guardian Security Standards.

3. Personal data⁵

Use of personal information	
Why would it not be possible to do without personal data?	The objective of the solution is to improve patient care through enhanced data sharing. It would not be possible to provide the outcome without the enhanced sharing of information for the purposes of direct care.
Please confirm that you will be using only the minimum amount of personal data that is necessary.	Yes
Would it be possible for the Controller/s to use pseudonymised ⁶ data for any element of the processing?	<div>Yes</div> <div><input type="checkbox"/></div> <div>No</div> <div><input checked="" type="checkbox"/></div>
If Yes, please specify the element(s) and describe the pseudonymisation technique(s) that you are proposing to use and how you will prevent any re-identification of individuals. (If you will be using the NEL pseudonymisation tool, simply enter: "NEL pseudonymisation tool", no further information is required).	N/A

Description of data: National and local data flows containing personal and identifiable personal information. What are the required personal data items?			
Personal Data	Please tick all that apply	Special Category Data	Please tick all that apply
Name	<input checked="" type="checkbox"/>	Racial / ethnic origin	<input checked="" type="checkbox"/>
Address (home or business)	<input checked="" type="checkbox"/>	Political opinions	<input type="checkbox"/>
Postcode	<input checked="" type="checkbox"/>	Religious beliefs	<input checked="" type="checkbox"/>
NHS No	<input checked="" type="checkbox"/>	Trade union membership	<input type="checkbox"/>
Email address	<input type="checkbox"/>	Physical or mental health	<input checked="" type="checkbox"/>
Date of birth	<input checked="" type="checkbox"/>	Sexual life	<input checked="" type="checkbox"/>
Payroll number	<input type="checkbox"/>	Criminal offences	<input type="checkbox"/>
Driving Licence [shows date of birth and first part of surname]	<input type="checkbox"/>	Biometrics; DNA profile, fingerprints	<input type="checkbox"/>
		Bank, financial or credit card details	<input type="checkbox"/>
		Mother's maiden name	<input type="checkbox"/>
		National Insurance number	<input type="checkbox"/>
		Tax, benefit or pension Records	<input type="checkbox"/>

⁵ 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.


⁶ 'pseudonymised' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

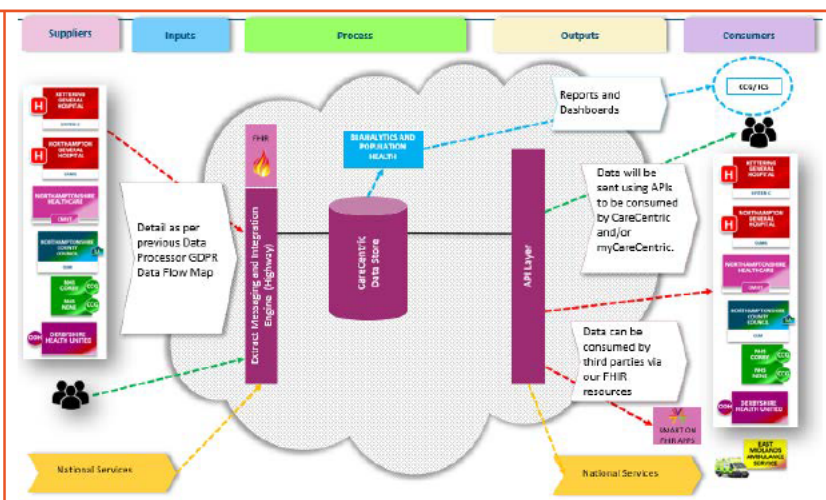
Please supply a dummy sample, e.g. blank forms or an itemised list of the data items.	Health, adoption, employment, school, Social Services, housing records	<input checked="" type="checkbox"/>
	Child Protection	<input checked="" type="checkbox"/>
	Safeguarding Adults	<input checked="" type="checkbox"/>
Additional data types (if relevant)		

Lawfulness of the processing			
Conditions for processing for special categories: to be identified as whether they apply			
Condition	Please tick all that apply		
Explicit consent unless or allowed by other legal route	Explicit consent	<input type="checkbox"/>	Other legal route <input checked="" type="checkbox"/>
Processing is required by law		<input type="checkbox"/>	
Processing is required to protect the vital interests of the person		<input type="checkbox"/>	
Processing is necessary for the performance of a contract		<input type="checkbox"/>	
Processing is necessary to perform a task in the public interest		<input type="checkbox"/>	
Processing is necessary for a legitimate interest or the legitimate interests of a third party		<input type="checkbox"/>	
Is any processing going to be by a not for profit organisation, e.g. a Charity		<input type="checkbox"/>	
Would any processing use data already in the public domain?		<input type="checkbox"/>	
Could the data being processed be required for the defence of a legal claim?		<input type="checkbox"/>	
Would the data be made available publicly, subject to ensuring no-one can be identified from the data?		<input type="checkbox"/>	
Is the processing for a medical purpose?		<input checked="" type="checkbox"/>	
Would the data be made available publicly, for public health reasons?		<input type="checkbox"/>	
Will any of the data being processed be made available for research purposes?		<input type="checkbox"/>	

The answers will not specifically identify the legality of the data flow; your responses to the questions below need to identify the specific legal route for processing. You will need to identify the legal basis using the GDPR article 6 (for personal data) and article 9 (for special category data) conditions met, as referenced in Chapter 2, section 8 and 10 of the Data Protection Act 2018.

The IG Team are available to help you identify the legal route for processing data.

Describe the information flows	
The collection, use and deletion of personal data must be documented.	
<p>Does any data flow in identifiable form? If so, from which organisation, and to which organisation/s?</p> <p>Please include a data flow map and confirm the flow has been added to your Information Asset and Data flow register.</p>	<p>Data will be extracted, transferred and loaded in encrypted form and will not be transferred in identifiable format.</p> <p>DATA FLOW MAP</p> <p> GN_Northampton% 20DFM.xlsx</p>

	
<p>Media used for data flow?</p> <p>(e.g. email, post, courier, secure electronic means [e.g. SFTP], other – please specify all that will be used)</p>	<p>View of data from primary care systems (EMIS and SystmOne) will use the MIG for a real time visibility of data that has not yet been transferred into Care Centric.</p> <p>CareCentric looks up data on the MIG using HTTPS and relies on the MIG interfaces setting the security parameters.</p> <p>Data is transferred from the EMIS and SystmOne systems to CareCentric using SFTP secure encrypted transport.</p> <p>REF: DFM will be used to transfer the data between source systems across other NHCP organisations Service users only through single sign-on or user name & password to access the data securely.</p>

Answer all the questions below for the processing of Personal Confidential Data

What is the legal basis for the processing of identifiable data? Please identify the conditions under the Data Protection Act 2018 or the Section 251 approval under the NHS Act 2006– please include the approval reference number.

(See Appendix 1 for Legal basis under the

The lawful basis under the General Data Protection Regulation will be:

- Articles 6(1)(e) (public task) and 9(2)(h) (medical purposes); or
- Articles 6(1)(d) (vital interests) and 9(2)(c) (vital interests)

Under the Common Law Duty of Confidence, information can be shared for direct care purposes with implied consent when there is a

Answer all the questions below for the processing of Personal Confidential Data

Data Protection Legislation)

Please include a copy of your consent form and identify when and how will this be obtained and recorded?⁷

reasonable expectation.

The GMC Confidentiality Guidance states at paragraph 29 that there may not be a reasonable expectation in a shared care record scheme, so a decision will have to be made regarding whether implied consent or explicit consent is used to meet common law. It is proposed that implied consent will be used to meet the common law obligations, with adequate safeguards in place. Paragraph 28 of the GMC Code of Confidentiality states that implied consent can be used if four conditions are met, these being:

- a. *You are accessing the information to provide or support the individual patient's direct care or are satisfied that the person you are sharing the information with is accessing or receiving it for this purpose. This information is only being provided to clinicians to facilitate direct care, and it will mandated it cannot be used for other purposes*
- b. *Information is readily available to patients, explaining how their information will be used and that they have the right to object. This can be provided in leaflets and posters, on websites, and face to face. It should be tailored to patients' identified communication requirements as far as practicable.*

A fair processing campaign will be undertaken using various avenues of media to ensure all patients are aware of this project and the benefits and risks of it to them.

- c. *You have no reason to believe the patient has objected.*

Patients will have the right to opt-out of secondary data processing in line with the National Data Opt-out. How to opt-out of secondary processing in full alignment the National Data Opt Out will form a core part of the fair processing campaign.

- d. *You are satisfied that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect.*

⁷ See [NHS Confidentiality Code of Practice](#) Annex C for guidance on where consent should be gained. NHS Act 2006 s251 approval is authorised by the National Information Governance Board Ethics and Confidentiality Committee and a reference number should be provided

Answer all the questions below for the processing of Personal Confidential Data

	<p>Information will only be shared with clinicians or staff who have a duty of confidence through contractual terms or through the nature of their work. The CareCentric solution enables full audit capability, including transparency of what an individual employee has searched for and seen on any given date and time, as well as which individual employees across multiple organisations have accessed a specific citizens information.</p> <p>This approach was discussed at the Northants Data Governance Forum (NDGF) and an implied consent model under the Common Law Duty of Confidence was decided upon. This is clearly described in the Overarching Data Sharing Framework for Direct Care, under which this DPIA and agreement sits. This also fully aligns with the IG Framework for Local Health and Care Records (LCHR) issued by NHS England.</p>
Where and how will this data be stored?	<p>Each data controller will be responsible for the appropriate storage and access to the care data being shared, in line with DPA 2018 and GDPR 2016. Some of the information is available in read-only format from clinical systems, and the information will not be stored locally or written back to the source systems.</p> <p>The CareCentric solution is hosted in Microsoft Azure data centres which are certified to Cyber Essentials Plus, ISO27001, ISO27017 and ISO 27018: https://docs.microsoft.com/en-GB/microsoft-365/compliance/offering-home?view=o365-worldwide</p> <p>The data stored on media encrypted to the 256-bit AES standard.</p>
Who will be able to access identifiable data?	<p>Those clinicians undertaking direct care, support staff working under the direct supervision of professionally regulated staff and administrative staff employed by the data controllers in line with their role specific access.</p> <p>Those individuals with additional responsibility across the system for safe guarding in line with their specific role will have enhanced access to information. Specific individuals with responsibility for monitoring system access for data governance purposes will also have access to the system.</p>

Answer all the questions below for the processing of Personal Confidential Data

How will you ensure the accuracy of the personal data (including their rectification or erasure where necessary)?	<p>Information transferred for the purpose of direct care will be subject to the regulatory professional standards of record keeping, which includes accuracy. Where a data subject would like to have a clinical record corrected, the standard process of enabling a subsequent rectification of data will be followed.</p> <p>Data quality is the responsibility under existing data protection legislation of each data controller. Where it is apparent that data quality is an issue within one organisation or within one particular system, the Data Controller(s) will be notified and improvement monitored by the Executive Data Committee, and operationally managed through the Northants Data Governance Forum.</p>
How will you monitor and maintain the quality of the personal data?	The information transferred for direct care will be subject to the regulatory professional standards of record keeping, which includes accuracy. Data quality audits will remain under the control of each data controller as it is currently. All organisations using the CareCentric platform will achieve standards met on their annual Data Security and Protection Toolkit.
Will the data be linked with any other data collections?	SDRS as a flow of data will form the PMI for the primary care data feed; the NHS number, first name, surname and DOB will identify if source systems have a match against those terms. If there is a match, the records held in the originating systems become permanently linked unless manually separated.
How will this linkage be achieved?	The link is automatic against the fields NHS number, surname, first name and DOB.
Is there a legal basis for these linkages? i.e. is the Controller/s responsible for the data expected to co-operate/link data to carry out their legal obligations.	Without linking the data held across multiple systems for each individual data subject, the care record will not be complete. Vital aspects of an individual's health and care record would not be available which would negatively impact on the ability to deliver care safely. The data is linked as described in the data flow map (above).
How have you ensured that the right to data portability can be respected? i.e. Data relating to particular people can be extracted for transfer to another Controller, at the request of the person to which it relates, subject to: <ul style="list-style-type: none"> • Receipt of written instructions from the person to which the data relates. 	<p>The information held within the NCR is held by multiple data controllers and the data subject can request for the transfer of their medical records in line with each organisations process at the time of request.</p> <p>The digital transfer of an individual's entire health and care record to another provider, for example when moving to a different area, is not yet technically feasible. This capability is on the solutions roadmap but</p>

Answer all the questions below for the processing of Personal Confidential Data

<ul style="list-style-type: none"> Including data used for any automated processing, <p>And</p> <p>The transfer of the data has been made technically feasible.</p> <p>N.B. Transferable data does not include any data that is in the public domain at the time of the request.</p> <p>No data that may affect the rights of someone other than the person making the request can be included.</p>	<p>is not currently possible.</p>
<p>What security measures will be used when the data is in transit?</p>	<p>Data in transit is secured by encryption using certificates with SHA256 2048 bit algorithms.</p>
<p>What confidentiality and security measures will be used to store the data?</p>	<p>Data held in CareCentric is stored in UK based Microsoft Azure datacentres encrypted at rest to 256-bit AES standard.</p> <p>CareCentric has fully auditable access control which enables the continual monitoring of access to the data held within NCR. This drills down to an individual level, and links to the Active Directory or authentication system of contributing organisations.</p> <p>Role Based Access Control (RBAC) will fully manage the visibility of data stored within the system at all levels, including system access roles. A mandated Starter & Leaver process for all organisations using the NCR will ensure that RBAC remains effective.</p> <p>Password management has a minimum standard of 8 characters with a mix of numerical/ letter/ symbol standards.</p> <p>Single sign-on is used where possible to ensure a contextual relationship exists with a patient prior to accessing their shared care record.</p> <p>A planned programme of education, training and reminder for all staff using the NCR will complement the current mandatory IG training across the system. This will ensure that staff are continually aware of their responsibilities in accessing the data.</p> <p>Contractual requirements between data controllers and processors will provide a strong legal framework to ensure the ongoing security of data held within the system at rest.</p>

Answer all the questions below for the processing of Personal Confidential Data

How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?

The clinical data transferred for the purpose of direct care will be subject to the 2016 Records Management Code of Practice (see link below)

[Records Management Code of Practice for Health and Social Care 2016](#)

At the end of the contract to provide the NCR, there is a clear contractual arrangement for the secure and timely transfer of data to an alternative supplier if required. The exit strategy has been evaluated and clearly meets the required standards. The retention periods will fully align with national data retention schedules.

What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?

Confidentiality :

Graphnet do not routinely share information with third parties and would only do so with the express permission of the customer.

Security

Where in-context launch within a specific health or care system is not possible, the user will be given access to a secure web-enabled portal, controlled via organisationally-managed role based access controls. In this scenario, those individuals will be required to identify themselves with a username and strong password. NCR use can be fully audited by user, and reports/audit is available for the purposes of monitoring appropriate/inappropriate access.

Web API calls (real time data retrieval): All requests and responses are done over HTTPS (Hypertext Transfer Protocol Secure) on the N3 network between Graphnet and third-party partners (who are covered in the Data Sharing Framework For Direct Care, this DPIA and accompanying Schedule 2).

An example is Healthcare Gateway and their MIG Service for GP data. Access to The Northamptonshire Care Record will be available to the majority of users via their existing health or social care record system. Therefore, only users with legitimate access to the health or care system will be able to see the Northamptonshire Care Record.

Appropriate use of data:

Access to data held within the NCR will be strictly governed by the Northants Data Governance Forum, overseen by the Northamptonshire Health and Care Partnership's Executive Data Committee.

Answer all the questions below for the processing of Personal Confidential Data

	<p>Any secondary processing of data held within the NCR will be subject to a full Data Protection Impact Assessment and Purpose Specific Information Sharing Agreement (PSISA) in line with the legislative requirements. This will be subject to scrutiny by all data controllers contributing to the NCR. Approved data flows will be added to the Data Flow Map held within the document and embedded within the PSISA and DPIA for the new processing.</p>	
<p>Please confirm you have a System Level Security Policy (SLSP) for the project/service.</p> <p>This policy needs to identify the technical controls that enable you to demonstrate that you have ensured privacy by design has been addressed by ensuring you have information on the controls required to protect the data.</p>	<p>No</p>	<p>Data Processor (Graphnet) complies with ISO27001 and aligns with ISO27018 and therefore CareCentric this includes controls covering:</p> <ul style="list-style-type: none"> • authentication includes strong passwords and password lockout • RBAC access control • system recovery and resilience, backups and BCP/DR • anti-virus • firewall protection and network segregation • patching and updates to assets • data encryption in transit and at rest • asset monitoring and alerting • application and infrastructure audit trail and logging • multifactor authentication for technical support staff • All organisations involved with the use of CareCentric will achieve standards met on the Data Security and Protection Toolkit.
<p>If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA?</p> <p>Is there functionality to respect objections/ withdrawals of consent?</p>	<p>Each data controller has an agreed Subject Access Request process which is fully compliant with the DPA 2018 and GDPR 2016. The information contained within the Care Plan section of the NCR will be appropriately redacted and issued by the Data Controller receiving the request. All organisations involved with the use of CareCentric will achieve standards met on the Data Security and Protection Toolkit.</p>	
<p>Are there any plans to allow the information to be used elsewhere either in the wider NHS or by a third party?</p>	<p>The NCR will sit alongside the Northamptonshire Analytics Reporting Platform (NARP) once it has been procured (planned 2020/21). This will run the Population Health Management tool, and when processing occurs for the purpose of Direct Care, the Northants Care Record may contribute data for that purpose.</p> <p>When the NARP and Population Health Management Tool are procured, this document will be revised to reflect any changes to the use of the data held within the NCR. The approval routes will be maintained in that each data controller will be fully engaged in the</p>	

Answer all the questions below for the processing of Personal Confidential Data

	<p>review and sign-off process.</p> <p>The procurement of the Personal Health Record will enable key data held within the NCR to be made visible to individual data subjects. This work will be covered by a separate PSISA and DPIA, but the data flow map held within this DPIA will be updated to reflect the changes introduced.</p>
<p>Will the privacy notices in relation to this data be updated and ensure it includes:</p> <ul style="list-style-type: none"> • ID of controller • Legal basis for the processing • Categories of personal data • Recipients, sources or categories of recipients of the data: any sharing or transfers of the data (including to other countries) • Any automated decision making • Retention period for the personal data • Existence of data subject rights, including access to their data and/or withdrawal of consent and data portability 	<p>An over-arching Privacy Notice for the purpose of Direct Care for Northamptonshire Health and Care Partner organisations has been drafted and will be available through a link on each data controller's website. Each data controller who signs the agreement will be listed in the Privacy Notice.</p> <p>A separate Privacy Notice for the Northamptonshire Care Record will be available.</p> <div data-bbox="687 925 754 987" data-label="Image"> </div> <p>NCR PN.docx</p>
<p>Where consent is the legal basis/there is automated processing. The data must be able to be easily separated from other datasets to enable data portability (see previous questions), audit of data relating to specific organisations and to facilitate any requirements for service transitions.</p> <p>Please describe how you will meet this requirement.</p>	<p>Consent is not the legal basis for the Northamptonshire Care Record. In addition, automated processing is not part of the NCR technical solution.</p>

4. Access and reporting

What access controls will you have in place to ensure there is only authorised access to the location the data is stored? Please include your procedure for enabling, monitoring access and identifying any inappropriate access.

Fully configured role-based access control will be in place linked to authentication and single sign-on from existing clinical systems to ensure a legitimate relationship between the staff and citizen.

Where direct user login is required, those individuals will be required to identify themselves with a username and strong password, with clear authenticated employment with an organisation signed up to the Overarching Data Sharing Framework for Direct Care, and cited on this DPIA and associated PSISA.

Additionally, Graphnet's technical support staff are required to use Multi-Factor Authentication to access the Azure environment. This ensures full transparency and control over access to the data by Graphnet's own staff, adding a layer of security.

Access to the system will be routinely audited and monitored by each data controller. The outcomes of all audits will be presented on a monthly basis to Northants Data Governance Forum. Inappropriate access to information held within the NCR will be managed alongside the Standard Operating Procedure for Incident Management as defined by the Data Security and Protection Toolkit. This includes the use of Serious and Untoward Incident reporting processes, which are reported to Northamptonshire CCG's Quality and Safety team in line with provider contract clauses.

Are there any new or additional reporting requirements from the system/software being used for this project/service? Yes/No

Yes

If "No" move to section 5 below: Business Continuity planning

What roles will be able to run reports? E.g. service activity reports, reports on individual people.

The Information Governance teams within each provider organisation will have NCR access in order to be able to run access audit reports and incident investigations. All staff accessing the NCR will be given clear information relating to access audits and the monitoring capability of the CareCentric solution. Additional reminder pop-ups will give staff an additional reminder that their actions are visible and audited regularly. All incidents involving the NCR will be managed in a consistent approach through a common agreed standard, approved by HR within each organisation

What roles will receive the report or where will it be published?

The IG Teams for each organisation will be able to generate and review their own NCR Access Audit Report, which will be disseminated at the appropriate internal governance committee. These reports will be presented monthly at the Northants Data Governance Forum for scrutiny and trend analysis. In addition, data breaches will be discussed and action plans developed in line with DSPT requirements. Individual data breaches will also be reported and managed through the Quality Team within Northamptonshire CCG in line with current contractual requirements.

Aggregated reports will be provided to EDC and all Serious Untoward Incidents will be presented and discussed at that Committee. Appropriate action, including escalation to the Northamptonshire Health and Care Partnership Executive Board will be taken as necessary.

Will the reports be in person-identifiable, pseudonymised or anonymised format?

Person-identifiable reports will be generated for internal audit purposes. Anonymised access reports to NDGF will be provided, with the caveat that trend analysis may require identification of individuals for serious incidents. Fully anonymised reports will be provided to the Executive Data Committee, unless required to do so for serious incident management.

Will the reports be in sensitive or redacted format (removing anything which is sensitive) format?

The Access Audit Reports will be in redacted format as appropriate. Where an investigation is required, the minimum amount of personal data will be used to ensure that the investigation is robust, in line with the associated agreed Incident Management Policy.

If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?

Yes/No

Yes

What plans are in place in relation to the internal reporting of a personal data breach?

(NB Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual(s), it will normally need to be reported to the ICO within 72 hours.)

All personal data breaches will be managed in line with the Data Security and Protection Toolkit requirements as mandated by NHS Digital. This includes the requirement to report to the ICO within 72 hours of detection, and the mandated notification of other data controllers involved in the data breach.

What plans are in place in relation to the notification of data subjects should there be a personal data breach?

(NB Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s), they should be notified as soon as reasonably feasible and provided with any recommendations to mitigate potential adverse effects.)

The Data Controller for the organisation under which the personal data breach has occurred will have responsibility for notifying the data subject of the personal data breach as soon as reasonably practicable. The Data Controller will also be responsible for leading the incident investigation and providing a Root Cause Analysis to the CCG's Quality Team and the Executive Data Committee. The Executive Data Committee will provide a summary report of findings including lessons learnt to the Northamptonshire Health and Care Partnership Board to ensure robust and transparent reporting of all serious incidents at Chief Executive level.

As a processor, Graphnet is contractually obliged to notify Northamptonshire CCG within 24hrs of detecting a data breach. There is an agreed Standard Operating Procedure for this between Graphnet and Northamptonshire CCG.

5. Business continuity planning

How will the personal data be restored in a

In summary, personal data would be restored by recovering

timely manner in the event of a physical or technical incident?

from a backup taken during the previous night's backup routine. Graphnet would then work with source suppliers to replay any messages received since the backup, using a combination of replay and stored messages within the interface.

Graphnet has full Business Continuity Plans and Return to Normal Operations plans, which have been scrutinised as part of the procurement process prior to contract award. Graphnet is fully DSPT compliant with annual BCP testing to ensure currency.

6. Direct marketing⁸

Will any personal data be processed for direct marketing purposes?

Yes/No

No

If Yes, please describe how the proposed direct marketing will take place:

7. Automated processing

Will the processing result in a decision being made about the data subject solely because of automated processing⁹ (including profiling¹⁰)?

Yes/No

No

If Yes, is the decision:

- necessary for entering into, or performance of, a contract between the data subject and a data controller
- authorised by law
- based on the data subject's explicit consent?

Please describe the logic involved in any automated decision-making.

⁸ direct marketing is "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations

⁹ examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention

¹⁰ 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

8. Risk Management and action plan

The risk score will determine the level of authorisation needed for any DPIA completed that requires a full DPIA. Any risk score that is verified by the IG team to be in the upper range of a medium risk score (9 to 12) or in the range of high risk will require referral to the NEL Data Protection Officer for review and approval. Any DPIA risks that score as high risk will only have the processing of the data approved once the risk has either mitigated to reduce the risk to medium as a minimum or where this is not possible, a high-risk score will require escalation to NHS England and approval from the Information Commissioner's Office before any processing can commence. The escalation process also includes a review to enable the risk to be lowered to within tolerance, if possible. The table below identifies the ranges for the scores and the risk level associated with each range of scores.

Risk level	Score
Low Risk	1 to 6
Medium	7 to 12
High	13 to 25

The risk assessment tool used is dependent on the data processed and the source of the risk involved. There is an information asset risk scoring tool available and embedded below, a security risk assessment tool is available where the ICT infrastructure poses the highest risk. If the dependency of the service/project is strongly linked to a particular service with its own risk scoring tool, such as Clinical Services, then that tool will be used to assess the risk and include the information asset risk score as a factor to the assessment.

Data Protection Risks

List any identified risks to Data Protection and personal information of which the project is currently aware. Risks should also be included on the project risk register.

Risk Description (to individuals, to the NEL CSU or to wider compliance)	Current Impact	Current Likelihood	Risk Score (I x L)	Proposed Risk solution (Mitigation)	Is the risk reduced, transferred, or accepted? Please specify.	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Inappropriate access to NCR records	3	2	6	Significant communication campaign to educated staff regarding inappropriate access to NCR, including consequences; full and regular access audits, discussed monthly and escalation process	Reduced	Yes

				in pace		
Cyber security risks	5	1	5	The CareCentric platform and Azure cloud storage have appropriate and significant technical security measures in place; each data controller is required to comply with Data Security and Protection Toolkit standards;	Significantly reduced	Yes; all organisations contributing data to or viewing data within the NCR are mandated to be DSPT compliant;
Data controllers and processors do not have sufficient IG controls in place to provide other data controllers assurance regarding the handling of personal data	3	3	9	All participants with the NCR are mandated to submit DSPT standards met annually.	Significantly reduced	
Data quality, including accuracy	2	3	6	Each data controller has responsibility for the quality and accuracy of data flowing into the NCR.	Reduced	
IG Teams have insufficient resources to run audit reports	4	3	12	The audit functionality of CareCentric enables reports to be run as a standard, minimising the time required to run an audit report	Reduced	

Approval by IG Team/Information Security

Risk Description	Approved solution	Approved by	Date of approval

Actions to be taken

Action to be taken	Date of Completion	Action Owner
DPIA completed for review by partner organisation DPO's		

9. Conclusions

Consultation requirements

Part of any project is consultation with stakeholders and other parties. In addition to those indicated "Key information, above", please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information. Where a lead Commissioner/Controller has been identified that organisation must consult with, capture actions from and gain approval from all collaborating partners.

It is the project/service lead's responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations.

Further information/Attachments

Please provide any further information that will help in determining Data Protection impact.

See Appendix 2, note 5 for examples

IG Team comments:

The DPIA has been completed in conjunction with the Digital Lead for Northamptonshire Clinical Commissioning Group, Graphnet's technical security and information governance team and has been subject to peer review by an IG SME within NEL's IG team. The DPO's for each partner organisation will be able to comment individually when signing off this DPIA.

Following review of this DPIA by the Information Governance Team, a determination will be made regarding the Data Protection impact and how the impact will be handled. This will fall into three categories:

1. No action is required by IG excepting the logging of the Screening Questions for recording purposes.
2. The questionnaire shows use of personal information but in ways that do not need direct IG involvement – IG may ask to be kept updated at key project milestones.
3. The questionnaire shows significant use of personal information requiring IG involvement via a report and/or involvement in the project to ensure compliance.

IG peer review

IG staff name: [REDACTED]

Signature:

Date: 17/07/2020

Please email entire completed document to nelcsu.Information-Governance@nhs.net

The lead Commissioner/Controller SIRO is responsible for ensuring all collaborating partner SIROs have approved the DPIA before signing on their behalf (if needed) below. If in doubt, the procurement or project manager must consult with the SIRO from each collaborating partner. Consultations that relate to risk mitigation must be reflected in the action planning section and capture actions and related approvals from all stakeholders, to capture the collaborative view of risks and issues before signing the DPIA below.

SIRO approval

SIRO name:

Signature:

Date:

Data Protection Officer (DPO) approval

DPO name:

Signature:

Date: