Updated May 2022

Kent & Medway
Care Record

DATA PROTECTION IMPACT ASSESSMENT

FOR

KENT AND MEDWAY CARE RECORD (KMCR)

relating to the coordinated provision of direct care across health and social care services and settings in Kent and Medway through the KMCR

Version	Date	Purpose	Author
1.0	28/08/2020	Initial draft	MJM
1.1	01/09/2020	Information required by organisations for completion of DPIA highlighted for action	MJM
1.2	03/09/2020	Compliance with UK GDPR Art 9 2 (b)(h) added (Page 3) (Page 8) Rewording of anonymisation statement (Page 3) Rewording of Disengagement statement (Page18) Summary statement added to Section A	MJM
1.3	04/09/2020	Comments from PE for review: Removal of criminal offence data as not required	MJM
1.4	10/09/2020	Review from HO'N Expansion of Project summary to include need for subsequent DPIAs for next wave(s) and research Removal of This will also be visible to others involved in their care and to the individual themselves where they access their Personal Health Record. From Section E: 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? as not relevant to first wave Review from GS: Will information about individuals be disclosed to organisations or people who have not previously had routine access to it? Response changed to Yes Section D Checked box is for Other legal route. Box for Explicit Consent had been removed and has been re-inserted Review from KA: Under Religious beliefs Yes (where it may impact healthcare choices) Review from DA: Detail removed from Does this project use new technologies or AI as response is No Terminology correction in line with other documentation	MJM
1.5	16/09/2020	HO'N review Page 5 response to *Will this match data or combine datasets from different sources or collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')* National Data Opt-out reference removed and changed to: The notice contains clear and sufficient information on the applicable legal basis for processing under this DPIA and information regarding how to register an objection to information being used on KMCR.	MJM
1.6	25/09/2020	Review following production of Crib Sheet / Glossary for consistency and terminology	MJM
1.7	29/09/2020	Review for consistency and typos etc.	SH
1.8	02/10/20	Updated for final review. Terminologies, definitions, and duplications corrected. Document reformatted, renumbered, and inconsistent terms changed or deleted in line with aligned intentions of contributors and stakeholders References to first and second waves removed.	TAA
1.9	13/10/2020	Incorporated contributions from stakeholders	TAA/SH
1.10	29/10/2020	Final – KMCR Board Approved	SH
1.11	01/11/2020	Final - KMCR Board Approved plus reference to Criminal Record data	SH
1.12	02/02/2021	Updated to include use of Live Patient Data for Systems User Acceptance Testing (UAT)	SH

Version	Date	Purpose	Author
1.13	05/04/2021	Updates to incorporate Secondary Use of Data for Population Health Management (PHM)	SH
2.0	13/04/2021	Updated to include clarity in respect of secondary use of data for Population Health Management - approved at IGWG.	AJ/EW
3.0	02/09/2021	Updated to reflect changes to templates following introduction of eforms to KMCR and rights of connected parties. Approved at August 2021 governance meetings.	AJ
3.1	20/04/2022	Updates following transition to BaU	CA
4.0	22/07/22	Approved at Board	CA

KMCR Data Protection Impact Assessment (DPIA)

Introduction

The Data Protection Impact Assessment (DPIA) is a process designed to systemically analyse, identify and minimise impact of a project or process on data protection and privacy.

An effective DPIA will help to identify the most effective way to comply with Data Protection obligations and meet individuals' expectations of privacy allowing the organisation to identify and resolve any problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

Who is responsible for approving and managing the risks identified within a DPIA?

This DPIA is the template created and approved by the Kent Medway Commissioning Group on behalf of all KMCR Data Controllers ("Joint Controllers"). The DPIA must be reviewed, updated as necessary, accepted and formally recorded and assigned by each Joint Controller and the data protection/privacy risks managed and owned by the KMCR Joint Controller organisation before the processing starts.

Once the risks relating to a project /process have been identified, the Joint Controller must ensure that appropriate safeguards – organisations and technical measures are implemented to meet the requirements of the UK GDPR and Data Protection Act in order to protect the rights and freedoms of the Data Subjects.

Full Data Protection Impact Assessment (DPIA)

SECTION A

Project name:	Kent and Medway Care Record (KMCR) Project	
Project lead	**Name**	Kent and Medway Clinical Commissioning Group, (CCG) Kent County Council, Medway Council and Kent Community Health NHS Foundation Trust (KCHFT) ("Commissioners") represented by KCHFT as lead commissioner.
	Designation	Statutory duty to commission health care service for Kent and Medway.
	Telephone	
	Email	
Information Asset Owner (if different to above)	The Project involves multiple organisations. Information Asset Owner will be appointed by each Joint Controller in its Joint Controller Agreement.	
Date:	28th August 2020	
Project Summary	The Kent & Medway Care Record (KMCR) is an Electronic Care Record that links data held in different provider systems for the purpose of providing health and care. The service will provide the essential infrastructure for integrated care through frictionless patient data-sharing. It will not be possible to deliver integrated care across the Kent and Medway County or execute the NHS Long-Term Plan, without a single shared care record. Graphnet, the provider, has its own bespoke solution; 'CareCentric' which allows it to reconcile Data Subject's Data from numerous data sources across Kent and Medway, ensuring that a single view of a Data Subject's record is available to authorised health and social care professionals, and practitioners, involved in a Data Subject's care and support. Without the use of KMCR, there is a risk of silo-based decision making, negatively impacting on care planning, and ultimately impacting on the service user. This DPIA covers the use of the KMCR for the purposes of direct care; any additional use of data from or within the KMCR will be addressed in its own DPIA. The Kent and Medway Clinical Commissioning Group, Kent County Council, Medway Council and Kent Community Health NHS Foundation Trust (KCHFT) commissioned System C healthcare Ltd to provide the KMCR using Graphnet Health Ltd's CareCentric through the KMCR Contract thereby appointing Graphnet as the Processor for the KMCR.	

	The Commissioners and the Controllers listed in section B below are hereinafter jointly referred to as "Joint Controllers" and separately as "Commissioners" and "Controller". Meaning of all undefined terms are contained in the KMCR IG Glossary available upon request. With appropriate agreements in place, numerous local data sets will be incorporated, such as feeds from Acute, Community Trusts, General Practices, Social Care, other local government services, and third sector partner data, which will allow the KMCR to provide enhanced joined up care. Data flowing into the KMCR is delivered in real time for the acute trusts, via HL7 transfer and via automated download every 24 hours for all other partner organisations, ensuring an up to date, holistic review of the patient's record.

SECTION B

Data Protection impact assessment (DPIA) screening questions				
Name and short description of project and data sets to be used:				
Will this project lead to:	Yes	No	Unsure	Comments
Will the project compel individuals to provide information about themselves		No		The KMCR Project will use Confidential Patient Information (CPI), i.e. Personal Data and Special Categories of Personal Data, already held by Controllers and continues to be provided to, or become available to Controllers who will subscribe to the KMCR, in the 'ordinary course of business'.
Are you using information about individuals for a new purpose or in a new way that is different from any existing use?		No		Personal Data and Special Categories of Personal Data, will be used in line with the provisions of s251(b) of the Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015. This provision created a statutory 'duty to share' information held about an individual with others involved in their care and treatment where it is likely to facilitate provision of their health and social care.
Will the project result in you making decisions about individuals in ways which may have a significant impact on them?		No		The statutory 'duty to share' requires health or social care organisations to share health records they hold about individuals with others involved in their care. This aligns with public expectations and does not over-step the boundaries of reasonable expectation of Data Subjects. Data Subjects are citizens accessing and/or using health, care, social care or wellbeing services in Kent or Medway, including but not

				limited to patients, social care service users and care service users.
Will the project require you to contact individuals in ways which they may find intrusive?		No		There will be no change in the contact to individuals as all Health and Social Care staff with access to KMCR data will do so in the course of their duties and direct care of citizens.
Does the project involve multiple organisations?	Yes			The KMCR is a project initiated by the Kent and Medway Sustainable Transformation Partnership (KMSTP) Digital Workstream. The KMCR is commissioned by the Kent and Medway Clinical Commissioning Group, Kent County Council, Medway Council and Kent Community Health NHS Foundation Trust (KCHFT) with KCHFT appointed as Lead Commissioner (for the purpose of implementation and management) by the Commissioners. Controllers will include: I. Kent and Medway GP Practices II. Social Care Providers III. Mental Health Trusts IV. Community Care Providers V. Acute Trusts VI. Emergency Care Providers VII. Kent and Medway Hospices A full list of Controllers can be found in Section F with the list of GP Practices provided as Annexure D and Hospices in Annexure E.
Does the project involve new or significantly changed handling of a considerable amount of personal data/special category data about each individual in a database?	Yes			Personal Data, Special Categories of Personal Data which relates to Data Subject's health, care, social care or wellbeing, including their detailed treatment or clinical or care history will be processed to fulfil the statutory duty to share. While the processing of data remains for the purposes of direct care, the use of a centralised platform and its associated feeds, including increased access to partner organisations, would indicate the significantly changed handling of data. Further, in recognition of the KMCR as a dynamic service, the completion of this and associated DPIAs, ensures Joint

				Controllers are meeting their requirements to fulfil the provision of Art 35 of GDPR.
The use of special category, including criminal offence data, on a large scale or in a new way	Yes			Personal Data, Special Categories of Personal Data which relates to Data Subject's health, care, social care or wellbeing, including their detailed treatment or clinical or care history will be processed to fulfil the statutory duty to share. However, the processing of data across Kent and Medway health and care system would constitute large scale processing as is a requirement of the KMCR. Appropriate safeguards and access controls have been put in place to enable this processing.
Will this profile individuals on a large scale such as tracking individuals' location or behaviour		No		The KMCR aims to give those involved in a Data Subject's care and support, access to digital health records held by others involved in their care. The aim is to allow right information to the right person at the right time. Processing for direct care purposes will not include profiling or tracking of individuals' behaviours.
Will this process biometric data; process genetic data		No		No biometric data is processed via KMCR.
Will this match data or combine datasets from different sources or collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')		No		Data will only be combined and/or matched from sources who are involved in a Data Subject's care within the Kent and Medway area. Nonetheless, the Privacy (Fair Processing) Notice for each joint data controller is published and available to Data Subjects. The notice contains clear and sufficient information on the applicable legal basis for processing under this DPIA and information regarding how to register an objection to information being used on KMCR. Data Subjects may exercise their rights by contacting the designated KMCR IG lead and in accordance with the advice provided by the Information Commissioner's Office (ICO) at www.ico.org.
Will this profile children or target marketing or online services at them		No		No profiling will be involved in the processing for direct care purposes.
Will this process data that might endanger the individual's physical health or safety in the event of a security breach	Yes			Data flowing through the KMCR will include all health and social care data including for example safeguarding information. By the nature of such

				sensitive data, there are increased risks in the event of a security breach. The KMCR is provided by System C Healthcare Ltd using Graphnet Health Ltd (“Graphnet”) CareCentric. Graphnet as Processor will comply with the highest data security standards to process CPI. Graphnet operates under a contractual obligation of confidentiality and is fully compliant with the requirements of the Data Security and Protection Toolkit. Graphnet is independently certified and audited to International Organisation for Standardisation (ISO)’s ISO:27001 (information security standard) and approved by NHSE/I.
Does this project use new technologies or AI		No		
Will this lead to systematically monitoring of publicly accessible places on a large scale (i.e. CCTV)		No		
Will this project result in the profiling of special category data to decide on access to services		No		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to it?	Yes			Currently, authorised health and social care professionals and practitioners involved in a Data Subject’s care and support will have access to relevant parts of the Data Subject’s combined record. Each access will be logged and automatically link the professional who is caring for that individual. This will be visible to others involved in their care. Access to relevant elements of a patient’s record will be strictly limited on a ‘need to know’ basis using KMCR Role Based Access Controls (RBAC) which will be aligned to the National RBAC. KMCR RBAC Policy is attached as Annexure B. All users must work for, and on behalf of, at least one of the KMCR Connected Parties. However, the essence of the KMCR is to act as an Integrated Digital Care Record (IDCR) providing joined-up care to Data Subject within the Kent and Medway area not to provide access to data to individuals who do not require it.

SECTION C

Use of personal information			
Description of data: National and local data flows containing personal and identifiable personal information			
Personal Data	**Please tick all that apply**	**Sensitive Personal Data**	**Please tick all that apply**
Name	Yes	Racial / ethnic origin	Yes
Address (home or business)	Yes	Political opinions	N/A
Postcode	Yes	Religious beliefs	Yes (where it may impact healthcare choices)
NHS No	Yes	Trade union membership	N/A
Email address	Yes	Physical or mental health	Yes
Date of birth	Yes	Sexual life	Yes
Payroll number	N/A	Criminal offences	Yes
Driving Licence [shows date of birth and first part of surname]	N/A	Biometrics and genetic data	N/A
		Fingerprints	N/A
		Bank, financial or credit card details	N/A
		Mother's maiden name	N/A
		National Insurance number	N/A
		Tax, benefit or pension Records	N/A
		Adoption	Yes
		Child Protection	Yes
		Safeguarding Adults	Yes
Additional data types (if relevant)		The KMCR is not limited by the National data sets. Detailed specification of data sets is attached as Annexure B. For clarification, the National data set was not used for the creation of the KMCR. The KMCR consumes data set specifications specific to the individual Controller Personal Data feed.	

SECTION D

<table>
<tr><th colspan="6">Lawfulness of the processing</th></tr>
<tr><th colspan="6">Conditions for processing for special categories: to be identified as whether they apply</th></tr>
<tr><th colspan="3">Condition</th><th colspan="3">Please tick all that apply</th></tr>
<tr><td>State legal route chosen</td><td>Explicit consent</td><td>☐</td><td>Other legal route</td><td>☒</td><td></td></tr>
<tr><td colspan="5">Processing is required by law</td><td>Yes</td></tr>
<tr><td colspan="5">Processing is required to protect the vital interests of the person</td><td>Yes</td></tr>
<tr><td colspan="5">Is any processing going to be by a not for profit organisation, e.g. a Charity</td><td>N/A</td></tr>
<tr><td colspan="5">Would any processing use data already in the public domain?</td><td>N/A</td></tr>
<tr><td colspan="5">Could the data being processed be required for the defence of a legal claim?</td><td>N/A</td></tr>
<tr><td colspan="5">Would the data be made available publicly, subject to ensuring no-one can be identified from the data?</td><td>N/A</td></tr>
<tr><td colspan="5">Is the processing for a medical purpose?</td><td>Yes</td></tr>
<tr><td colspan="5">Would the data be made available publicly, for public health reasons?</td><td>Yes</td></tr>
<tr><td colspan="5">Will any of the data being processed be made available for research purposes?</td><td>Data processed under this DPIA for the purposes of direct care will not be made available for research purposes. Any requests to process data for research purposes will following the Secondary Use Policy and Operating Procedure and will be accompanied by the Secondary Use DPIA and any additional DPIAs required for its specific purpose.</td></tr>
<tr><td colspan="5">Will data be used to support Population Health Management (“PHM”) activities by and across partner organisations of the KMCR programme?
• Use of data to design new models of proactive care and deliver improvements in health and wellbeing – a by-product as a result of data sharing for direct care
• De-identified information from the records is to be used for real-time decision making to support the delivery of PHM approaches.
• Make better use of de-identified information from people’s health and care records to understand more about health and disease, improve public health for the population, develop new treatments, monitor safety, and plan and deliver health and social care services more effectively.
• The KMCR will provide a platform to explore the potential for use of data – in an anonymised form – to support other functions such as research.</td><td>Data will be processed in accordance with UK GDPR Article 9(2)(h) Necessary for the provision of health and/or social care and the management of health or social care systems & services in so far as it meets the criteria for direct care processing.
All other uses of identifiable data (e.g. risk stratification) will be subject to specific approval based on an appropriate legal basis for use, such as section 251 of the National Health Service Act 2006 and will be detailed within their associated DPIA (see the DPIA for Secondary Use Processing for further details).</td></tr>
</table>

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.

SECTION E

Answer all the questions below for the processing of Personal Confidential Data	
What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?	Inclusion of identifiable data is necessary to provide individual patient and service-user care in the provision of integrated care. Using identifiable data will ensure that the correct Data Subject has been identified so that the correct clinical history is obtained to provide the best care to such Data Subject. Some personal data may also be collected for data subjects who are not patients, but are instead connected individuals being relatives, professionals or others relating to provision of care services, protection of their welfare or acting as an emergency contact. Personal Data which qualifies as Special Categories of Data under Article 9(1) of the UK General Data Protection Regulation ("UK GDPR") and Sections 10(1) and 11(1) of the Data Protection Act 2018 ("DPA") will be processed in fulfilment of the Joint Controller's legal obligation.

What is the legal basis for the processing of identifiable data? e.g. Conditions under the Data Protection Act 2018, the Section 251 under the NHS Act 2006 etc.	Lawfulness of processing is based on the fulfilment of a legal obligation (Article 6(1)(c) UK GDPR) as detailed in the Health and Social Care Act 2012 s251(b) (as amended by the Health and Social Care (Safety and Quality) Act 2015 which created a statutory 'duty to share' information amongst relevant commissioners and providers for the purposes of direct care and commissioning. Processing is further carried out under the lawfulness conditions of vital interests as in (Article 6(1)(d) and the performance of a public task (Article 6(1)(e)) of the UK GDPR. **Article 6(1)(c) Legal Obligation:** *the processing is necessary for you to comply with the law (not including contractual obligations).* **Article 6(1)(d) Vital Interest:** *processing is necessary in order to protect the vital interests of the data subject or of another natural person.* **Article 6(1)(e) Public Task**: *the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.* Special Categories of Data to be processed has met the exceptions listed under Article 9(2)(b) and 9(2)(h) of the UK GDPR subject to the conditions set out in Article 9(3) of the UK GDPR and s11(1) and 204 of the DPA. **Article 9(2)(b) Legal Obligation:** *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;* **Article 9(2)(h) Direct Care and Administration:** *processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards.* Criminal offence data is limited to that which relates to Data Subjects' health or care, a comprehensive register of criminal convictions will not be kept and the condition of Article 10 of the UK GDPR as well as s10(5) of the DPA 2018 has been fulfilled. **Article 10 Criminal Convictions and Offences:** *Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.*

	Consent of Data Subjects is not relied on, as Data Subjects will be fully informed of how their data is being used under Article 6(3). The conditions and safeguards enumerated in Schedule 1 Part 1 in Sections 2(2) (c), (d), (e) and (f) of the DPA have been met. The statutory 'duty to share' requires health or social care organisations to share health records they hold about individuals with others involved in their care. This aligns with public expectations and does not over-step the boundaries of reasonable expectation.
Where and how will this data be stored?	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 The data stored on media encrypted to the 256-bit AES standard.
Who will be able to access identifiable data?	Health and social care professionals in the provision of integrated direct care. Authorised health and social care professionals and practitioners involved in a Data Subject's care and support will have access to relevant parts of the Data Subject's combined record. Each access will be logged and automatically link the professional who is caring for that individual. This will be visible to others involved in their care and to the individual themselves where they access their Personal Health Record. Access to relevant elements of a Data Subject's record will be strictly limited on a 'need to know' basis using the KMCR Role Based Access Controls (RBAC) which will be aligned to the National RBAC. All Users must work for, and on behalf of, at least one of the Onboarded Connected Parties. Compliance of Onboarded Connected Parties with UK GDPR Art 9 2(b) and (h) will ensure the safeguarding of children and vulnerable adults who are at risk. The sharing of care records will allow improved identification of those at risk, enabling care decisions to be better informed and reducing the level of risk. This includes interoperability with the Integrated Child Protection System. Specific individuals with responsibility for monitoring system access for data governance purposes may have access to the system user logs, but not specific patient datasets.
Will the data be linked with any other data collections?	The KMCR builds on existing shared care record tools namely the Medical Interoperability Gateway (MIG), Care Plan Management System (CPMS), Egton Medical Information Systems (EMIS) and Vision and Microtest systems. NHS number, first name, surname and DoB will be used to link the source systems to the KMCR records.

What security measures will be used to transfer the data? Is this in line with cyber security requirements	The technical platform for data transfer is the CareCentric product from Graphnet CareCentric is a secure system that allows secure cross boundary access to patient information held in the shared records. CareCentric can pull data from multiple systems, including GPs, Acute Trusts, Community Trusts, Local Authorities, Mental Health Trusts, Out of Hours Services, Ambulance Services, Social Care systems and bring them together in a single patient record. These records are then displayed in one place for both staff and patients for the provision of integrated care. Graphnet is fully compliant with the requirements of the Data Security and Protection (DSP)Toolkit, independently certified and audited to ISO:27001 (information security standard) and approved by NHSE/I. Existing commercial agreements between system provider(s) and Graphnet, means data can be transferred to the KMCR without needing to install local software. To protect data in transit, Graphnet's CareCentric uses Microsoft Azure Service. Azure implements the transmission integrity and confidentiality control by ensuring that cryptography is implemented through a hybrid model. The following is a high-level list of the symmetric and asymmetric cryptography models used for encrypting and protecting confidentiality of data. • Use 256-bit (Advanced Encryption Standard) AES for symmetric encryption/decryption • Use 128-bit or better symmetric keys • Use RSA for asymmetric encryption/decryption and signatures • Use 2048-bit or better RSA keys • Use Secure Hash Algorithm (SHA) SHA-256 or better (SHA-384, SHA512) for hashing and • message authentication codes. In addition, Azure has implemented cryptography in the following ways: • Communications between the Azure service offerings and the Microsoft Azure Management Portal are protected with the use of Transport Layer Security (TLS) 1.2. • Hardware Security Modules used by the Key Vault service employ Federal Information processing Standards (FIPS) 140-2 validated encryption. Azure is assessed to ISO 27001, ISO 27017, ISO 27018, and many other internationally recognized standards. The scope and proof of certification and assessment reports are published on the Azure Trust Center section for ISO certification here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001.

	The ISO 27001 assessment was performed by the British Standards Institution (BSi). • Data in transit between end user device(s) and the application is protected using TLS 1.2. • Data in transit within the application is also encrypted using TLS 1.2. • Data in transit is protected between the service and other services (e.g. where APIs are exposed) using TLS 1.2. All the above encryption is mandatory. CareCentric is designed with security in mind and uses Transport Layer Security (TLS) 1.2 (or later) with 2,048-bit RSA/SHA256 encryption keys to encrypt data in transit both within the application and externally with the application and its Data Protection Application Programming Interface DPAPIs, as recommended by CESG/NCSC.

What confidentiality and security measures will be used to store the data?	Graphnet is registered and compliant with the DSP Toolkit, located with its Organisation Data Service (ODS) Code 8GX89. The DSP Toolkit covers in detail the measures and policies Graphnet has in place to assure that it is meeting the Data Quality principles of Confidentiality, Integrity and Availability. Further information about any aspect of the DSP submission can be made available upon request. Further, Graphnet is certified to ISO27001:2013 and undergoes regular independent audits from an external United Kingdom Accreditation Service (UKAS) certified auditor (BSi) to ensure continued compliance to this standard and also ISO 9001:2015. Additionally, Graphnet holds the Cyber Essentials Plus certification and is working towards ISO 27018. CareCentric is designed with security in mind and uses Transport Layer Security (TLS) 1.2 (or later) with 2,048-bit RSA/SHA256 encryption keys to encrypt data in transit both within the application and externally with the application and its Data Protection Application Programming Interface DPAPIs. Data at rest is also encrypted and Graphnet only store this data in UK based Microsoft datacentres through Microsoft Azure Cloud. Graphnet is considered by Microsoft to be a Cloud Customer to them and as a business has no direct or hands-on access to any Microsoft locations or hardware. Microsoft have however worked closely with Graphnet to ensure that the data centres used during its collaboration with Microsoft are within the UK. The Microsoft Azure cloud computing platform meets a broad set of international and industry-specific compliance standards, such as ISO/IEC (International Electrotechnical Commission) 27001/27002:2013, Health Insurance Portability and accountability Act (HIPAA) and Federal Risk and Authorisation Management Program (FedRAMP). Microsoft adheres to the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers. For day to day protection, anti-malware systems are in use throughout Graphnet and within the application environment. The application uses a Web Application Firewall protecting it against the Open Web Application Security Project (OWASP) "Top 10".
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	Retention periods shall be as set out in NHS Records Management Code of Practice 2021 which can be found at NHSX_Records_Management_CoP_V7.pdf Additionally, Graphnet will retain data in line with the KMCR Contract terms and conditions.

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?	KMCR Clinical and Professional Reference Group (CRPG) will determine the data sets necessary for each 'use-case' or clinical pathway and access to relevant elements of a patient's record will be strictly limited on a 'need to know' basis using KMCR Role Based Access Controls (RBAC) which will be aligned to the National RBAC. All users must work for, and on behalf of, at least one of the Onboarded Connected Parties. Each access will be logged and automatically link the professional who is caring for that individual. Single sign-on is used where possible to ensure a contextual relationship exists with a patient prior to accessing their shared care record. As it concerns Graphnet who is the Processor, the impact of potential or actual data breach situations are all assessed by the IG/IS/ISO team (legal counsel, Data Protection Officer and Security Manager) in line with Graphnet's risk management process (ISO27001:2013 certified). Graphnet have a robust incident management procedure in place to respond to any security incidents: the IG/IS and ISO management team will assess issues and monitor progress on the action taken to ensure corrective action is taken. Broadly speaking, the process is: a. Incidents/issues shall be raised on JIRA GQS (Grey Quality System) service desk and allocated an individual reference number: any employee may add an issue. b. The management team will close the issue/incident when satisfied that acceptable corrective action(s) has been taken by the relevant data controller. c. Escalation of a ticket directly to senior members of the IG/ISO Steering committee will be used for significant issues. These will be progressed and closed as detailed below. The IG/IS/ISO management team will monitor investigations and actions taken to ensure appropriate corrective action is taken, e.g. update policies/procedure, risk assessment. When the management team, and where required the Chief Technical Officer, is satisfied all possible actions have been taken, the issue shall be classed as resolved and the mitigation plan assessed for success for closure. All potential impacts and risks (financial, public perception, confidentiality etc.) are considered when a risk incident is reported. As the contractual Data Processor, Graphnet will notify the customer (Data Controller) within 24hours. KCHFT as Lead Commissioner have recruited a dedicated BaU team including IG specialist, contract manager and technical experts to support in the management and security of the system. Contractual requirements between Controllers and Processors will provide a strong legal framework to ensure the ongoing security of data held within the system at rest. Annual assurance checks will be conducted by the KCHFT KMCR BaU Team to ensure ongoing compliance with DSPT by all Controllers and Processors. Additional reviews and audits will be undertaken to ensure governance

	arrangements remain fit for purpose and that any regulatory changes have been incorporated into documented processes and procedures. Finally, representatives of the Joint Controllers and Graphnet are properly sanctioned and all systems are secure.
What rights will individuals have such as the right to object etc.	Regarding identifiable data necessary to provide individual patient and service-user care in the provision of integrated care, Data Subjects will have the following rights: i. to be informed ii. to get access to their data iii. to rectify or change data iv. to restrict or stop processing data v. object to data being processed or used Data Subjects will have the following rights under UK GDPR however, these are not absolute and may be overridden should there be legal grounds to do so: vi. erase or remove data vii. move, copy or transfer data viii. know if a decision was made by a computer rather than a person Where data is made available pursuant to the provisions of Section 254 or 259 of the Health and Social Care Act 2012 and the relevant provision of Schedule 1 Part 1 in Sections 2(2) of the DPA have been met, data subjects' rights will be upheld in all circumstances where there is not a legal necessity to override this interest. This will ordinarily mean compliance with the following rights: i. to be informed ii. to get access to their data iii. to rectify or change data Other data subjects e.g. connected individuals being relatives, professionals or others relating to provision of care services, protection of their welfare or acting as an emergency contact, will retain these rights. Privacy (Fair Processing) Notice for each Connected Party is published and available to Data Subjects. Notice contains clear and sufficient information on applicable rights of Data Subjects.
Is the National Opt-out (patients' consent) applicable to this process/service	National Opt-Out is indirectly applicable to the KMCR. How to Opt-Out or register an objection is contained in each Joint Data Controller's Privacy (Fair Processing) Notice. Data Subjects may exercise their rights through the KMCR nominated IG Lead and in accordance with the advice provided by the Information Commissioner's Office (ICO), www.ico.org .
Will the privacy notices need to be updated	Privacy Notices of all Onboarded Connected Parties may need to be updated where they do not sufficiently provide the information supplied by this DPIA.

Detail audit trails that can be run to ensure information is not used inappropriately	The KMCR initial screen view offers only limited demographic information, allowing health professionals to confirm the correct Data Subject before proceeding to the view patient record. The KMCR's user access logs record views and incidents are monitored locally by Controller organisations for suspicious behaviours. It generates user logs which can be audited by authorised users within each organisation, according to their assigned RBAC functionality. Accessing a record is associated with individual's care and this will be visible to other health professionals involved in their care. 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. Further, the KMCR includes an audit trail showing which user accessed a Data Subject's records. Access to the system will be routinely audited and monitored by each Controller. The summary outcomes of all audits will be presented to IGWG on an annual basis at minimum. Inappropriate access to information held within the KMCR should be escalated to KCHFT KMCR BaU team immediately and will be managed alongside the Standard Operating Procedure for Incident Management as defined by the Data Security and Protection Toolkit.

<u>Environmental Scan</u> **Consultation/checks that have been carried out regarding this process/service of similar nature, whether conducted within your organisation or by other organisations.** *Please provide any supporting documents if available*	A report was commissioned in October 2018 to gather public and patient feedback about the development and options for the KMCR. This was conducted by Engage Kent with the aims: • To increase awareness of the Kent & Medway Care Record using digital communication methods • To engage targeted sections of the general public across Kent and Medway and explore their thoughts and ideas about the concept of KMCR and what the public / patient might find useful to have included. • To generate a pool of informed and interested members of the public to create an engagement resource for the project as it moves forward. The full report is available here PDF Engage Report - Seldom Heard feedb A Citizens' Engagement Group is to be established and there are planned communications to: • Ensure awareness of the KMCR. • Ensure understanding of what the KMCR does, how it can be used and accessed, and how it is secure. • Deliver the message that the KMCR is useable, useful and widely used. • Ensure commitment and support for the project. • Set and manage expectations appropriately. • Encourage feedback, ongoing engagement and participation from stakeholders. • Effectively manage any potential risks or issues that occur relating to areas of work. • Communicate implementation timescales. • Reinforce the benefits of the Project and its outcomes

SECTION F

Core organisations need to review the table below and ensure:

1. The correct legal entity is identified
2. The relevant ICO registration number is correct or inserted
3. Compliance with Data Security and Protection Toolkit is entered as a Yes or No

If there are multiple organisations involved in processing the data list below? *If yes, list below*			Yes/No
Name	Controller (C) or Processor (P)?	Information Commissioner Office registration	Completed and compliant with the Data Security & Protection Toolkit[1]
			Yes/No
Graphnet Health Ltd; the sub-contracted provider of the contract holder System C Healthcare Ltd	P	Z1045461	Yes (20/21)
Kent and Medway Clinical Commissioning Group (CCG).	C	ZA703045	Yes (21/22)
Kent County Council (KCC)	C	Z5297748	Yes (20/21)
Medway Council	C	Z5895541	Yes (20/21)
Kent and Medway GP Practices	C	Please see Annexure D	Yes (20/21)
Kent Community Health NHS Foundation Trust (KCHFT)	C	Z2844951	Yes (20/21)
Dartford and Gravesham NHS Trust	C	Z4828025	Yes (20/21)
East Kent Hospitals University NHS Foundation Trust (EKHUFT)	C	Z9093025	Yes (20/21)
Medway Maritime Hospital - Medway NHS Foundation Trust	C	Z5002033	Yes (20/21)
Maidstone and Tunbridge Wells NHS Trust	C		Yes (20/21)
Kent and Medway NHS Social Care Partnership Trust (KMPT)	C	Z9417133	Yes (20/21)
North East London Foundation Trust	C	Z9096541	Yes (20/21)
HCRG Care Group	C	Z2823541	Yes (20/21)
Medway Community Healthcare	C	Z2614640	Yes (20/21)
South East Coast Ambulance NHS Trust	C	Z9509701	Yes
Integrated Care 24 Limited	C	Z956524X	Yes (20/21)

Kent and Medway Hospices	C	Please see Annexure E	Yes (20/21)
Has a data flow mapping exercise been undertaken? (please provide details)			Yes/No
			Yes, please see Annexure C for Data Flow Map

SECTION G

Review and Risk matrix

Are there any risks to the **Confidentiality** of personal data? *Confidentiality is defined as unauthorised disclosure of, or access to, personal data.*

i. Inadvertent disclosure: Inadvertent disclosure of identifiable personal data to viewing health/care professional who may not have the authorisation to view certain data sets or health/care professional may inadvertently pull record of an individual with whom they have no legitimate professional interest, where wrong or similar information to the intended patient is wrongly entered or associated with Data Subject’s care.

ii. Data Subject Right Infringement: Data Subject may misunderstand or misapply the provisions of UK GDPR as it concerns their individual rights. Data Subjects may believe that their rights to object to data being processed or used, erase, remove, or data portability, are being infringed upon.

iii. Malicious and unauthorised access or disclosure: Viewing health or care professional may maliciously pull record of an individual for their own interests using their authorised access.

iv. External Attack: Cyber-attack /Malicious software attack on Processor or any Joint Data Controller’s systems causing loss or disclosure of personal data. In the event of a security breach, processing of personal data may endanger Data Subject’s physical health or safety.

v. RBAC and Data Sets: Authorised KMCR user breaches the provision of KMCR RBAC. Failure of authorised users to comply with RBAC and access unauthorised data sets may result in confidentiality breach.

vi. Disengagement of Joint Data Controller or a previously authorised user from the KMCR: timeline within which access to the KMCR is restricted where a Connected Party terminates its use of the KMCR may affect confidentiality. Timeline within which access can be denied to a Joint Data Controller’s departing employee or authorised user may affect confidentiality. The effect on data flow where a Joint Data Controller disengages from the KMCR may affect confidentiality.

vii. KMCR Access: Due to its nature as a joined-up care record service, Data Subjects may be wary of wider reach and unlimited access to their personal data even when they become aware of KMCR RBAC policy. Risk of unauthorised user viewing personal data through an authorised user’s login while in the engagement of a Joint Data Controller or after their departure from the engagement of a Joint Data Controller but before disconnection from the KMCR.

viii. Involvement of multiple organisations: Processing will combine data or datasets from different sources or collect personal data from a source other than the Data Subject. Thus:

A. Where Joint Data Controller fails to update their privacy notice to reflect the KMCR, there may be a risk to confidentiality.

B. Data Subject may be unaware of the identity and which Connected party or Data Controller to contact to exercise their statutory rights under data protection law.

C. Connected Parties may vary how they express or may not express the purpose and legal basis of processing as it relates to the KMCR in ways that are concise, transparent, intelligible and easily accessible, using clear and plain language, in particular for information addressed specifically to a child.

ix. LINK WITH OTHER DATA COLLECTION SYSTEMS: KMCR builds on existing shared care record tools namely MIG, CPMS, EMIS and Vision and Microtest systems. Confidentiality risk may therefore arise where the implementation documentations for the use of data by these record sources are not compliant with current data protection laws or are set up to prevent the application (particularly the advantages) of current data protection laws.

Are there any risks to the **Integrity** of personal data? *Integrity is defined as unauthorised or accidental alteration of personal data.*

i. INCOMPLETE RECORD: Incomplete records or Lack of adequate and timely data flow from a Joint Data Controller(s), or where a Joint Data Controller's data cannot update into the KMCR within the timeline of other Controllers. Health or Care Professionals may therefore not be aware that a record is missing important information in these instances and assume they are viewing a complete record.

ii. CONTRADICTORY INFORMATION: Where the KMCR aggregates and presents contradictory information about a Data Subject in respect of similar data sets, health or social care professionals may find it difficult to decide which information is correct and current.

iii. KMCR VIEW: The records are view only and cannot be edited. However, Treatment Escalation Plans can be edited, and all changes are recorded, attributed to the editor.

iv. INVOLVEMENT OF MULTIPLE ORGANISATIONS: Input method(s) and choice of words of Onboarded Connected Parties may be differently expressed in respect of the same data sets.

v. CO-EXISTENT PAPER RECORDS: Previous records are not digital and the KMCR cannot extract records held on paper. Therefore, health professionals may diagnose or treat unaware of important clinical information because patient records accessed may be incomplete.

Are there any risks to the **Availability** of personal data? *Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.*

i. Partial or comprehensive unavailability of KMCRs at point of care.

Are there any known or immediate technical / IT / Information Security / Cyber Security concerns?

- There are no outstanding high or medium items from an ISO27001 point of view.
- There are no outstanding high or medium Cyber Essentials Plus points.
- No other known outstanding concerns that would affect Confidentiality, Integrity or Availability.

If the answer is "Yes" to any questions in this section, how are these to be reduced or mitigated?

MITIGATION TO CONFIDENTIALITY RISK

i. INADVERTENT DISCLOSURE: The KMCR landing page /initial screen view offers only limited demographic information, allowing authorised health or care professional to confirm correct Data Subject before proceeding to the record.

ii. DATA SUBJECT RIGHT INFRINGEMENT: Data is being processed as a legal obligation. Therefore, a reasonable Data Subject ought not to expect to have these rights. Data Subjects are being informed of their data protection rights in supporting resources particularly KMCR website (including other media communication as well as through Onboarded Connected Parties) and Privacy Notices. These include the means to object and how their objections will be handled by the KMCR administration. All Onboarded Connected Parties will be provided with model clauses for inclusion in their Privacy (Fair Processing) Notices.

iii. OTHER DATA SUBJECTS: Data being processed relating to other data subjects who are not patients, but are instead connected individuals, being relatives, professionals or others relating to provision of care services, protection of their welfare or acting as an emergency contact, is being processed under the legal basis of public task and the expectation under common law that this data is processed in the provision of care to data subjects. KMCR does not hold any information that would not be held within the individual care provider's own clinical records. These data subjects retain all rights that are afforded under UK GDPR, including the right to object.

iv. MALICIOUS AND UNAUTHORISED ACCESS OR DISCLOSURE: Incident/Breach (unlawful loss, disclosure or breach of personal data) will be considered and treated as an incident with consequential statutory reporting and notification obligations. KMCR has visible screen which includes a warning that accessing a record will associate health or care practitioner's access identity with a Data Subject's care record and this will be visible to other professionals involved in their care. KMCR is monitored for suspicious behaviours and generates access/user logs and record views, which can be audited. Incidents resulting from malicious and unauthorised disclosure will be referred to the Data Protection Officer of a Joint Data Controller responsible for user, to be dealt with according to the Joint Data Controller's incident management policy.

v. EXTERNAL ATTACK: Graphnet is fully compliant with the requirements of the Data Security and Protection Toolkit, is independently certified and audited to ISO:27001 (information security standard) and approved by NHSE/I. Anti-malware systems are in use throughout Graphnet and within the application environment for day to day protection. The application uses a Web Application Firewall protecting it against the OWASP "Top 10". Graphnet operate a data security plan which includes penetration testing routines and audits. KMCR Joint Controllers also agree interdependent loss/breach incident protocols that includes 'near-miss' reporting. Loss or disclosure of any volume of personal data resulting from cyber-attack will be treated as an incident. KMCR Joint Controllers will agree interdependent loss/breach incident protocols that includes 'near-miss' reporting. Responses to incidents will be coordinated by the KMCR IG Lead and the effected Controllers and communications with the Information Commissioner Office (ICO) will be managed in the first instance by the KMCR IG Lead. All Joint Controllers are required to observe and comply with the Data Security Principles particularly the Data Security and Protection Toolkit to ensure their protection is up to date, including annual penetration testing. Finally, representatives of System C, Graphnet and each Joint Controller are properly sanctioned, and all systems are secure. Therefore, there are no concerns over processing or security flaws.

vi. RBAC AND DATA SETS: Access to relevant elements of a Data Subject's record will be strictly limited on a 'need to know' basis using the KMCR RBAC which will be aligned to the National RBAC policy.

vii. DISENGAGEMENT OF A PREVIOUSLY AUTHORISED USER FROM THE KMCR: Each Joint Data Controller, as the responsible employer will be responsible for informing KMCR, at least monthly, of their Leavers, Movers and Changes where authorised users are concerned.

viii. KMCR ACCESS: Data Subjects also have the right to request a log of who has accessed their data and why and they also have the right to Opt-Out of the KMCR. Data Subjects are being informed and will continue to be informed of their rights and activities regarding the KMCR in supporting resources particularly KMCR website (and other media communication as well as through Onboarded Connected Parties) and Privacy Notices.

ix. INVOLVEMENT OF MULTIPLE ORGANISATIONS: Each KMCR Joint Data Controller is required to include KMCR clauses in their Privacy (Fair Processing) Notices. This will be done using ‘model clauses’ to be provided by the KMCR administration through KCHFT. KCHFT will also support each Joint Data Controller in responding to enquiries and /or data subjects exercising their rights and freedoms.

x. LINK WITH OTHER DATA COLLECTION SYSTEMS: The KMCR implementation documentations are being developed in a manner that ensures they can stand alone without reference to other data collection systems implementation documentations and compliant with current data protection laws.

MITIGATION TO INTEGRITY RISK

i. INCOMPLETE RECORD: Screen views will make the source of individual content items clear and show the organisation that provided them. It will also flag and provide a placeholder where data-items or records are being withheld or suppressed (e.g. due to patient objection being respected). This will include reminders that there may be information which the system is unaware of, e.g. out of area treatments, unconnected parties etc.

ii. CONTRADICTORY INFORMATION: All data is staged through a pipeline of data quality processes as data are ingested to ensure accurate matching and to provide the source and date of individual content items clear and show the organisation that provided them. In cases of conflict, Health or care professional is expected to exercise professional judgement and seek direct clarification from Data Subject where such Data Subject possesses the ability to make decisions at the point of treatment or through Data Subject’s representative. KMCR will have provision for updating or adding notes to the record. Over time, as mobilisation progresses, this risk should reduce.

iii. INVOLVEMENT OF MULTIPLE ORGANISATIONS: KMCR administration will continue to provide training on use of the KMCR. It is expected that transition to use of the KMCR will improve uniform entries by Joint Data Controller users.

iv. CO-EXISTENT PAPER RECORDS: Known paper information assets should be identified through audit of Onboarded Connected Parties Information Asset Registers and onscreen flags made available to professionals to enable them to exercise caution when considering their interactions with Data Subjects. Over time, digitisation of records is expected to reduce this risk.

v. PARALLEL NARRATIVE: Notes created through KMCR features will write back to Joint Data Controller’s record subject to appropriate controls and permissions.

MITIGATION TO AVAILABILITY RISK

i. The KMCR and platform (Microsoft) has availability of 99.99% in its Service Level Agreements. This may be compromised by interruptions to local or last-mile connectivity. Most connections are constantly monitored by the Kent CoIN service. Reporting of KMCR unavailability will be through each Joint Data Controller’s IT help desk, with second line support provided by KCHFT. Business Continuity

Plans will be triggered as applicable. If the outage is due to a natural disaster, Graphnet will initiate its Disaster Recovery Plan in accordance with operating procedures agreed with the KMCR administration.

Once the mitigations are implemented, how would you score any remaining risk in the following Risk Assessment? If you consider that there are no remaining risks give a value of 1 for both Likelihood and Severity.

Likelihood *(please tick)*			x	**Severity** *(please tick)*			=	9
1		Rare		**1**		Negligible		
2		Unlikely		**2**		Minor		
3		Possible		**3**		Moderate		
4		Likely		**4**		Major		
5		Almost certain		**5**		Catastrophic		

LIKELIHOOD	IMPACT / CONSEQUENCES				
	NEGLIGIBLE 1	LOW 2	MODERATE 3	SIGNIFICANT 4	EXTREME 5
1 (rare)	**L**	**L**	**M**	**H**	**H**
2 (unlikely)	**L**	**L**	**M**	**H**	**E**
3 (possible)	**L**	**M**	**H**	**E**	**E**
4 (likely)	**M**	**M**	**H**	**E**	**E**
5 (almost certain)	**M**	**H**	**E**	**E**	**E**

SECTION H

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 CCG 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?**
DATA CONTROL Lack of clarity over apportionment of data control responsibilities and accountabilities resulting in poor transparency and uncertainty over liabilities, risk ownership, indemnities.	4	2	8	Joint Controller Agreement and KMCR RBAC Policy ought to reduce this risk. These documents set out data control responsibilities and accountabilities.		Yes
INFORMATION ASSURANCE Confidential patient information may be disclosed to a User who is unable to demonstrate appropriate technical or organisational measures for data security and protection.	3	2	6	All KMCR Onboarded Connected Parties must complete an annual DSP Toolkit and achieve satisfactory or better or have in place an NHSD approved action plan. An audit of DSPT compliance will be undertaken on an annual basis.		Yes

KMCR USE CASES Use-cases are not clinically curated, validated and appropriately documented. To avoid undocumented changing purpose, or incremental extension of uses of the KMCR beyond stated purposes (i.e. individual care) and established lawful basis.	3	2	6	KMCRs approved used-cases and new purposes should be documented. Each must be subject to statutory sign-off by the nominated registered professional (profile) clinically curated as 'necessary and proportionate' and within the KMCRs documented information risk appetite. Project Team to develop a process with Graphnet (configuration management) for validating and documenting use-cases and creating UK GDPR compliant documentation (Art. 30 ROPA). Develop KMCR approval process. For each documented use-case, name the relevant UK GDPR Art.9(3) responsible clinician (Caldicott Guardian).	.	
RBAC, INAPPROPRIATE USER AND/OR PERMISSIONS Clinical, social work or administration staff have may have inappropriately elevated access roles or permissions, resulting in access to information they have no 'need to know'.	3	2	6	'Need to know' access permissions should be determined by the KMCR Clinical and Professional Reference Group during curation and creation of the applicable resource profile. These should be		Yes

				grouped according to professional boundaries.		
Duty of Transparency Failure to inform patients and service-users of KMCR purposes**.**	3	2	6	KMCR Privacy (Fair Processing) Notice model clauses to be drafted and updated in each Joint Data Controller's Privacy (Fair Processing) Notice.		Yes
Data Feeds from Controllers KMCR readiness for Controller data-feeds upload - Documentation reflecting the engagement of UK GDPR Article 28 has not been engaged by Controllers.	3	2	6	Required onboarding documentation to be executed between KMCR Commissioners, Graphnet and all other Controllers.		Yes
Failure to Comply Failure of one or more Joint Controllers to meet the minimum standards for DSPT compliance	3	2	6	All KMCR Onboarded Connected Parties must complete an annual DSP Toolkit and achieve satisfactory or better or have in place an NHSD approved action plan. A copy of the approved action plan and steps taken will be requested by the KMCR team and reviewed for updates in line with the agreed timeframes. An audit of DSPT compliance will be undertaken on an annual basis.		

SECTION I

Actions to be taken		
Action to be taken	**Date of Completion**	**Action Owner**
Appointment of Information Asset Owner by Controllers.	each Controller's sign up date.	Each Controller.
Controllers to confirm/supply correct legal entity, ICO registration and compliance with Data Protection and Security Toolkit	Controller sign up date.	Each Controller.
Privacy (Fair Processing) Notice for Onboarded Connected Parties to be drafted/updated and links for all Onboarded Connected Parties should be provided to KCHFT as lead commissioner.	Controller party go-live date.	Each Controller.
KMCR RBAC Policy to be attached as Annexure A	KMCR first go-live date.	KCHFT.
KMCR Data Sets to be agreed to meet the requirement of Section B	Completed	KMCR Clinical and Professional Reference Group
Confirmation of use of DSP Toolkit by each Controller.	Annually	KMCR IG Lead
Kent and Medway GP Practice's Information Commissioner Office registration to be provided in Annexure D	April 2022	Each Practice in Kent and Medway
Ensure functionality and update of KMCR page on KMCCG Website		KCHFT/KMCCG
Approved action plan from non-compliant Controllers requested and reviewed for assurance		KMCR IG Lead
Review and update all KMCR Agreements, Policies and Procedures for endorsement as a result of the move to BaU.	April 2022	KMCR IG Lead KMCR IGWG
More granular level Data Flow Map required for Annexure C		KMCR IG Lead Graphnet

SECTION J

Consultation requirements Consultation should be completed by the Project lead, should consultant be required by the ICO the Data Protection Officer will lead.
N/A

Information Governance team review Comments and Recommendations	
This DPIA has been reviewed and updated to reflect the current position of the KMCR service and the use of data for direct care only (removing all reference to secondary use processing as this is covered by a separate suite of documentation). A more detailed view of the data flows from each Controller system would strengthen assurance and provide clarity as to the processing of data.	
Reviewed by IG team	
Date and signature:	

SECTION K

DPO Comments and Recommendations	
DPO :	
Date and signature:	

SECTION L

SIGN OFF	
SIRO:	
Date & Signature:	
Caldicott:	
Date & Signature:	

Once completed, and signed off, please send this form to: kmccg.kmccg.ig@nhs.net

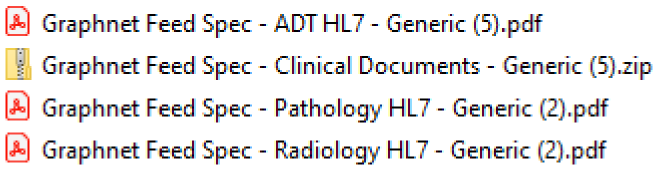
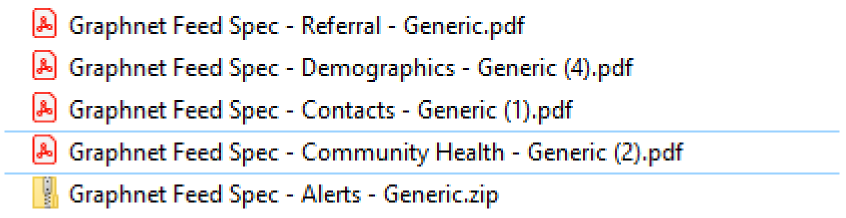
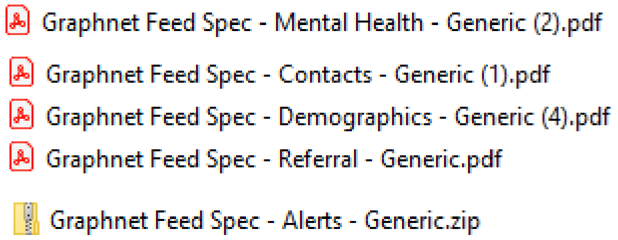
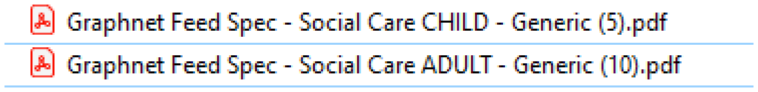
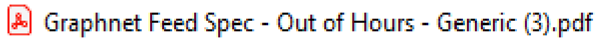
Annexure A

KMCR RBAC Policy

KMCR CareCentric
RBAC Policy v2.0 Clea

ANNEXURE B

KMCR DATA SETS

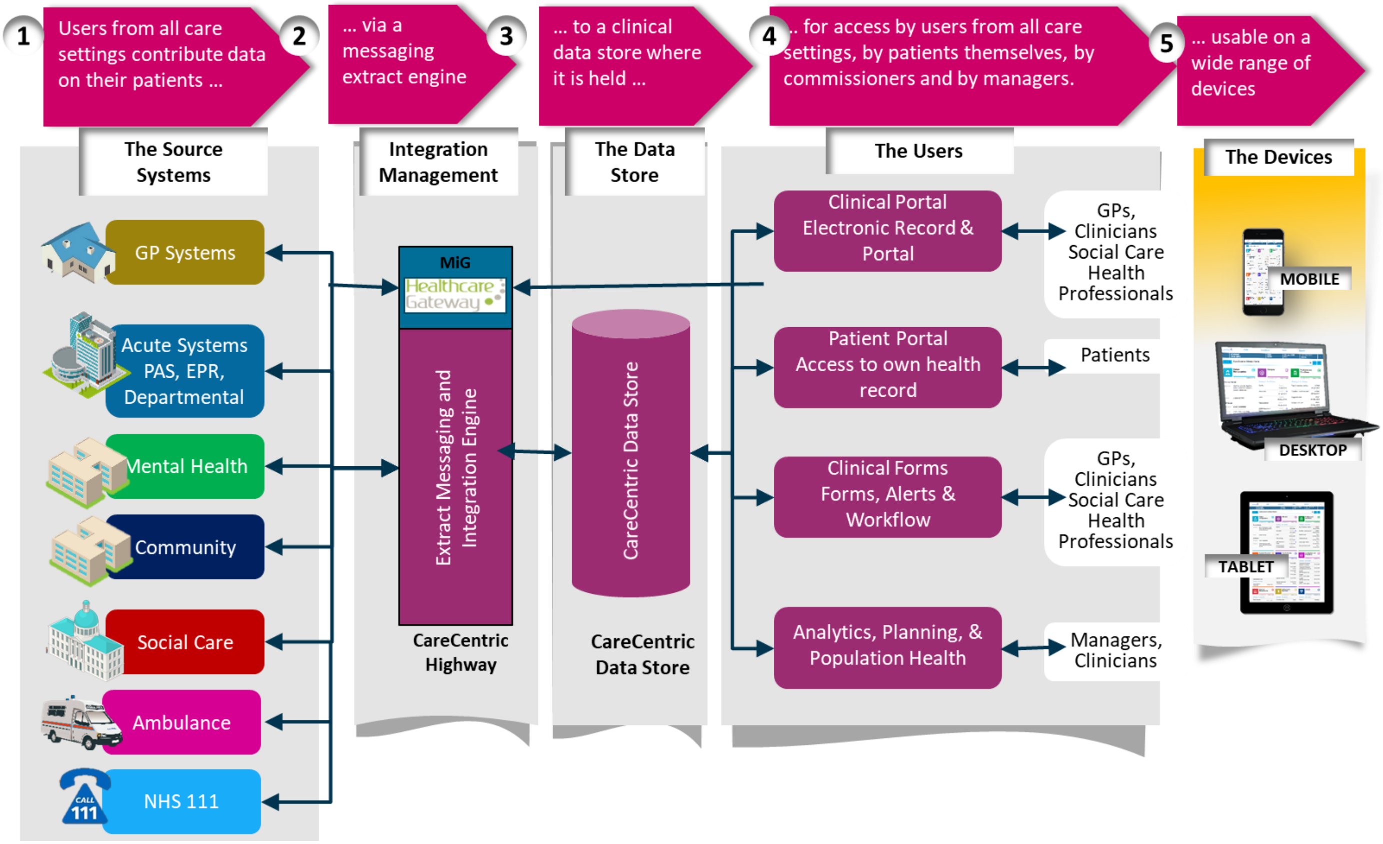
Data Feed	Specification
Acute	 Graphnet Feed Spec - ADT HL7 - Generic (5).pdf Graphnet Feed Spec - Clinical Documents - Generic (5).zip Graphnet Feed Spec - Pathology HL7 - Generic (2).pdf Graphnet Feed Spec - Radiology HL7 - Generic (2).pdf
Community	 Graphnet Feed Spec - Referral - Generic.pdf Graphnet Feed Spec - Demographics - Generic (4).pdf Graphnet Feed Spec - Contacts - Generic (1).pdf Graphnet Feed Spec - Community Health - Generic (2).pdf Graphnet Feed Spec - Alerts - Generic.zip
Mental Health	 Graphnet Feed Spec - Mental Health - Generic (2).pdf Graphnet Feed Spec - Contacts - Generic (1).pdf Graphnet Feed Spec - Demographics - Generic (4).pdf Graphnet Feed Spec - Referral - Generic.pdf Graphnet Feed Spec - Alerts - Generic.zip
Social Care	 Graphnet Feed Spec - Social Care CHILD - Generic (5).pdf Graphnet Feed Spec - Social Care ADULT - Generic (10).pdf
Out of Hours	 Graphnet Feed Spec - Out of Hours - Generic (3).pdf

Each Joint Controller should hold a copy of their complete feed specification for the data they flow into KMCR. KCHFT KMCR Team hold a copy of all data feed specifications as Lead Commissioner for the contract; any changes to feed specifications should be shared with the relevant Controllers and the KMCR Team as standard.

A full copy of the Graphnet Data Feed Specifications can be shared on request as necessary and appropriate.

Annexure C

KMCR Data Flow Map


1
Users from all care settings contribute data on their patients ...
2
... via a messaging extract engine
3
... to a clinical data store where it is held ...
4
.. for access by users from all care settings, by patients themselves, by commissioners and by managers.
5
... usable on a wide range of devices
The Source Systems
GP Systems
Acute Systems PAS, EPR, Departmental
Mental Health
Community
Social Care
Ambulance
NHS 111
Integration Management
MiG
Healthcare Gateway
Extract Messaging and Integration Engine
CareCentric Highway
The Data Store
CareCentric Data Store
CareCentric Data Store
The Users
Clinical Portal Electronic Record & Portal
GPs, Clinicians Social Care Health Professionals
Patient Portal Access to own health record
Patients
Clinical Forms Forms, Alerts & Workflow
GPs, Clinicians Social Care Health Professionals
Analytics, Planning, & Population Health
Managers, Clinicians
The Devices
MOBILE
DESKTOP
TABLET

Source Provider	Source Systems	Method of Transfer HL7/CSV etc.	Security
General Practice	EMIS Vision – Hosted Docman	CSV feed – automated daily transfer from source system to a dedicated port on the CareCentric infrastructure.	Secure File Transfer Protocol (SFTP)
Acute	Telepath Patient Centre Sunrise InfoFlex Apex Allscripts Symphony Telelogic	HL7 – real time transfer	Transport Layer Security (TLS) V1.2
Mental Health	RiO	CSV feed – automated daily transfer from source system to a dedicated port on the CareCentric infrastructure.	Secure File Transfer Protocol (SFTP)
Community	RiO EMIS EMIS Web	CSV feed – automated daily transfer from source system to a dedicated port on the CareCentric infrastructure.	Secure File Transfer Protocol (SFTP)
Social Care	Mosaic LiquidLogic	CSV feed – automated daily transfer from source system to a dedicated port on the CareCentric infrastructure.	Secure File Transfer Protocol (SFTP)
Ambulance	Cleric	CSV feed – automated daily transfer from source system to a dedicated port on the CareCentric infrastructure.	Secure File Transfer Protocol (SFTP)
Out of Hours	Adastra	CSV feed – automated daily transfer from source system to a	Secure File Transfer Protocol (SFTP)

		dedicated port on the CareCentric infrastructure.	
Hospice	EMIS iCare	CSV feed – automated daily transfer from source system to a dedicated port on the CareCentric infrastructure.	Secure File Transfer Protocol (SFTP)

ANNEXURE D

KENT AND MEDWAY GP PRACTICE'S INFORMATION COMMISSIONER OFFICE REGISTRATION AND DSPT COMPLIANCE

GP List with DSPT compliance and ICO

Annexure E

Kent and Medway Hospice's Information Commissioner Office registration and DSPT Compliance

Hospice List with
DSPT compliance an