Information Governance White Paper

EDGE Programme

Forward

Dear Subscriber

The research landscape within the UK continues to evolve; from April 2014 we will see the formation of 15 Local Clinical Research Networks in England. As part of the transition to this structure the NIHR has mandated the 15 local geographical networks to implement a common Local Portfolio Management System.

In addition to this, changes to regulatory frameworks within the EU and more stringent requirements on Trust to performance manage their research mean that it is more important than ever for institutions to fully understand their information governance responsibilities. Further it must be remembered that whilst the management of the studies may be performed at the LCRN level the obligations regarding information governance remain with the Trusts where the patient has been recruited/treated.

The practical application of these regulation in relation to the recording of information about research subjects and the use of systems such as EDGE remains as key to us as a supplier. As part of our commitment to our customers we have, therefore, commissioned a white paper to help us, and you, understand the requirements of the various government documents/guidance issued on the subject. The document also addresses how EDGE can assist in ensuring local trust compliance with the obligations identified.

We trust that you find the following useful and any feedback/comments can be contributed to the Ideascale thread on Information Governance.

Best Wishes

James Batchelor
Director EDGE Program

Document information

Title:	Information Governance White Paper
Commissioner:	The University of Southampton
Document owner:	James Batchelor
Document author:	Debbie Terry
Date created:	28/08/13
Current status:	FINAL Version 3
File name:	IG White Paper

Version history

Version	Date issued	Updated by	Reason
0.1	11/09/2013	Debbie Terry	Issued for comment
1.0	26/09/2013	Debbie Terry	Final version
2.0	26/09/2013	James Batchelor	EDGE Issued
2.1	21/12/2015	James Batchelor	Review of Piksel Carelink
2.2	21/12/2015	David Osler	Review of changes
3.0	22/12/2015	James Batchelor	EDGE Issued

Table of Contents

1 Introduction 3
2 Background Information 3
The Research Governance Framework 5
4 Information Governance 6
5 The Data Protection Act 1998 6
5.1 Data Controller and Data Processor Roles 6
5.2 The First DPA Principle – Fair and Lawful Processing 7
5.3 Lawful Processing 7
5.4 Fair processing 8
5.5 Schedule 2 condition 9
5.6 Schedule 3 condition 9
5.7 Processing Anonymised data 10
5.8 The Seventh DPA principle 11
5.9 The Contract 11
5.10 Information Security 11
5.11 Application Audit 12
5.12 Hosting Arrangements Information Security 13
6 NHS Act Section 251 14
6.1 Section 251 in relation to EDGE 15
7 Information Sharing with NIHR CRN 15
7.1 Anonymised data 15
7.2 Personal confidential data 15
8 List of Subscriber responsibilities: 18
9 Glossary 20

Appendix A: Master Services Agreement Schedule F Data Controller and Data Processor Contracts 22
Appendix B: List of Identifiable data items 28

1 Introduction

EDGE is an information system that supports collaborative clinical trials management and research studies. Clinicians and nurses conducting clinical trials or research studies enter personal data into the EDGE system and use it for case management purposes, including reporting in accordance with research governance requirements. The use of personal and sensitive personal data engages the Data Protection Act 1998 (the DPA) and privacy laws.

The uptake of the EDGE programme has encountered some problems and delays due to inconsistency in the interpretation of the legal and information governance requirements and a tendency for data controllers to be risk averse.

This EDGE Information Governance Guidance for Subscribers has been written to facilitate the implementation of EDGE by:

a) Explaining the legal and information governance requirements for the operation of the EDGE programme to provide pre-contractual advice to organisations wising to subscribe, and

b) To ensure that the subscriber organisations understand their data controllership responsibilities and ensure personal data processed in the system is lawful.

2 Background Information

EDGE is a software system developed by the University of Southampton (UOS) and University Hospitals Southampton NHS Foundation Trust (UHS) to support collaborative clinical trial management. UOS has (by agreement with UHS) the right to grant licences in respect of the System. UOS sub-contract Piksel Carelink who provide the managed technical hosting service.

The “EDGE programme” supports a wide range of research management functions, which empower research managers, data analysts, research nurses and clinicians to make the most of their information. By allowing organisations to actively manage research within a single system; information can be better organised and analysed in real-time. Multiple institutions can collaborate on a range of projects and reporting tools can help streamline the research governance and approval process[1].

[1] http://www.edgeclinicalresearch.com

Demographic data collection facilitated by EDGE allows NHS organisations to fulfil their duty of care to patients enrolled in clinical studies. The 2005 research governance framework for health and social care and the governance arrangements for research ethics committees, updated in 2012, set out standards for carrying out research in the NHS. The Research Governance Framework section 3.10 states that:

'it is the responsibility of organisations providing health or social care in England to be aware of all research undertaken in their organisation, or involving participants, organs, tissue or data obtained through the organisation.'

The National Institute for Health Research (NIHR) commissions and funds NHS, social care and public health research and the development of research evidence[2]. NIHR delegate certain functions to 15 Clinical Research Networks (NIHR CRN) across England[3], who are host organisations responsible for establishing and maintaining a local NHS clinical research infrastructure, providing funding and ensuring the delivery of a research management and governance service within their region.

NIHR CRN hosts have entered into an agreement with UOS on behalf of their local research organisations to establish Service Level Agreements for Local Portfolio Management System (LPMS) services under which they can become Subscribers to the System through a form of adherence and enter into a contract with UOS for services relating to the use of the System.

Subscribers, with support from UOS, will determine how they will set up and use the EDGE system to manage their clinical trials or research studies within the organisation.

The Clinician conducting the clinical trial or Researcher is responsible for ensuring that they follow the agreed research governance protocols and for protecting the integrity and confidentiality of clinical and other records or data generated during that study.

The EDGE licence arrangements also allows the NIHR CRN host to take an extract/feed of anonymised data generated/held in the System relating to English NIHR adopted trials for use in a Central Portfolio Management System.

The Strategy for UK Life Sciences[4] sets out the Government's ambition to strengthen and promote the life sciences industry. The NHS Mandate requires NHS England to ensure that the new commissioning system promotes and supports participation by NHS organisations and NHS patients in research to support the wider public interest in the innovation of medicine through clinical trials and research. The NHS Constitution includes a new commitment to inform people about research and to use anonymised information to support research.[5]

[2] http://www.nihr.ac.uk/research/Pages/default.aspx
[3] http://www.crncc.nihr.ac.uk/news/news_archive/new_local_hosts_announced_for_nihr_c+linical_research_network
[4] www.gov.uk/government/uploads/attchment_data/file/32457/11-1429-strategy for life-sciences.pdf
[5] https://www.gov.uk/government/publications/the-nhs-constitution-for-england

The NHS organisation subscribing to the EDGE system is responsible for ensuring that the clinical trial and research programmes conducted by their clinicians and nurses conform to the relevant protocols and lawful practice, which in addition to research governance includes information governance.

EDGE facilitates the collection and sharing of information, which includes the sharing of personal confidential data as well as aggregated and anonymised data therefore the Data Protection Act 1998, common law duty of confidentiality and the Human Rights Act 1998 (Article 8) are engaged.

3 The Research Governance Framework

The Research Governance Framework[6] is a framework of collective standards, systems and processes that govern the way in which medical research and clinical trials are setup and conducted to ensure compliance with national policy, ethics and law. It establishes a hierarchical structure of responsibilities,[7] which vary depending upon the type, size, scope etc. of the overall project, but are required to be set out in clear documented agreements for each study. Everyone involved in research with human participants, their organs, tissue or data is responsible for knowing and following the law and the principles of good practice relating to ethics, science, information, health and safety, and finance set out in this framework.

Researchers carry the day-to-day responsibility for the conduct of the research and in particular are responsible for ensuring that any research they undertake follows the agreed protocols and for protecting the integrity and confidentiality of clinical and other records and data generated by the research; and for reporting any failures in these respects, or suspected misconduct, through the appropriate systems.

EDGE is a dynamic software solution to problems often experienced in the management of clinical trials such as the collection of data on disparate or paper based systems.

By using the EDGE application an organisation can establish control and expect to:

- Manage portfolio, non-portfolio and commercial studies
- Track patient recruitment
- Track, monitor and audit research governance
- Act as a shared access secure data repository for users

[6] The Research Governance Framework : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/139565/dh_4122427.pdf

[7] Chapter 3

• Enable bespoke reporting on KPI's (e.g. time – to – target & patient recruitment)
• Provide a platform for improved resource management

4 Information Governance

Information Governance is the term used to describe the collective standards, systems and processes that govern the way in which information is handled within health and social care services to ensure compliance with national policy and the law.

Establishing good information governance standards will enable clinicians and research nurses to ensure their ethical and legal responsibilities for the protection, integrity and confidentiality of clinical and other records and data generated during the study are met.

Demographic data collection facilitated by EDGE allows NHS organisations to fulfill their duty of care to patients enrolled in clinical studies. EDGE enables clinicians and research nurses directly involved in the research or clinical trial to input all relevant data collected during the course of the study, allowing all staff involved to access one central securely held accurate record at the point of need.

EDGE also helps executive teams maintain effective oversight of research studies, ensuring they are properly resourced and managed. The result is better quality information and better research studies.

Use of the system involves the processing of personal and sensitive personal data (referred to collectively as personal confidential data or PCD) about their research participants; therefore the Data Protection Act 1998 (DPA) and privacy laws are engaged[8].

The following guidance explains the DPA arrangements within the EDGE system.

5 The Data Protection Act 1998

5.1 Data Controller and Data Processor Roles

The NHS Trust (or other research organisation) processing personal data and sensitive personal data about individuals participating in research and clinical trials is the Data Controller[9] under the terms of the Data Protection Act 1998.

[8] In addition to the DPA, the legal basis for processing personal data must also conform to common law duty of confidentiality and Human Rights Act 1998 (Article 8)
[9] See Data Protection Act 1998 Section 1 (1) for definition of Data Controller, Data Processor, personal data, sensitive personal data, processing and other terms.

A Data Controller is legally responsible for ensuring that all personal data they are responsible for is processed in accordance with the data protection principles, even when data processed on their behalf is processed by a Data Processor[10].

The Subscriber organisation Data Controller is responsible for assigning and managing their own staff's access rights to the system.

As part of the EDGE licence arrangements, UOS is acting as a Data Processor. UOS only handle anonymised data. UOS sub-contract Piksel Carelink to manage the IT hosting service that EDGE operates from. By holding personal data on the hosted servers and maintaining the system, Piksel Carelink is also a Data Processor.

The Subscriber is the Data Controller and legally responsible for ensuring that personal confidential data about their respective patients and held within the EDGE system is processed in accordance with the data protection principles. UOS and Piksel Carelink are Data Processors.

5.2 The First DPA Principle – Fair and Lawful Processing

The first DPA principle says that personal data must be processed fairly and lawfully and shall not be processed unless one of the conditions in Schedule 2 is met and, in the case of sensitive personal data[11] at least one of the conditions in Schedule 3 is also met[12].

This means that a data controller must:

- Have legitimate grounds for collecting and using personal and sensitive personal data;
- Be transparent and tell people how their data will be used;
- Not to use that data in ways that has unjustified adverse effects on the individual(s) concerned;
- Handle personal data in ways they would reasonably expect and understand; and
- Not do anything unlawful with the data

5.3 Lawful Processing

Lawful refers to other relevant statute and common law. Processing is unlawful if it involves committing a criminal offence or if it results in a breach of a duty of confidence; an

[10] DPA section 4(4)

[11] DPA Part 1 (2)

[12] DPA Schedule 1 Part 1 (1) (1st principle)

organisation exceeding its lawful powers or a breach of the Human Rights Act 1998 for example.

NHS Trusts are corporate bodies established under section 25 of the NHS Act 2006. Their lawful powers for conducting research and clinical trials are set out in Schedule 4, which includes undertaking and commissioning research (s16)[13].

Since May 2004 clinical trials conducted in the European Union are regulated under the EU Clinical Trials Directive[14] which regulates clinical trials on medicine to ensure the rights and safety of the individual patients participating in the trial are protected and the results of the trial are credible. The Medicines for Human Use (Clinical Trials) Regulations 2004 and Amendment 2006 establish the U.K research governance arrangements for clinical trials. Clinicians and nurses conducting clinical trials with a NHS Trust are legally required to record and provide information in accordance with those regulations (as well as other obligations).

The Health and Social Care Information Centre (HSCIC) are issued their "Guide to confidentiality in health and social care" on the 12th September 2013. The supporting reference document (Section 2) explains the common law duty of confidentiality and consent in detail. [15]

All health and social care organisations (or anybody working with them to provide services or care) processing confidential information in relation to the provision of publicly funded health or adult social care activities must have regards to the guide.

The NHS Organisation conducting the clinical trial or research study is responsible for ensuring that they have legitimate grounds for collecting and using personal and sensitive personal data and do not do anything unlawful with the data.

5.4 Fair processing

In addition to their research governance responsibilities for effectively informing patients about the intended clinical trial and research study as part of the recruitment process, clinicians and research nurses are also responsible for providing information about the intended use of their personal data (fair processing) and the patient's rights in that respect.

The basic legal requirement is to make sure people know who you are, what you intend to do with their personal data and who it will be disclosed to. The Information Commissioner's Privacy notices code of practice provides guidance about what to include in privacy or fair

[13] http://www.legislation.gov.uk/ukpga/2006/41/contents

[14] DIRECTIVE 2001/20/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use

[15] http://www.hscic.gov.uk/confguideorg

processing notices.[16] It is good practice to inform individual's that the organisation has entered into a contract with other organisations to provide health informatics services and to have information about those outsourcing arrangements available for patients who want to know more about this.

The HSCIC Guide (Rule3) All health and social care organisations should clearly explain to patients, service users and the public how confidential information they collect could be used in a de-identified form for research etc.

The NHS Organisation conducting the clinical trial or research study is responsible for ensuring that the patients recruited for a clinical trial or research study have been provided with fair processing information (privacy notices) that clearly explains what you intend to do with their personal data, who it will be disclosed to and the intention to use anonymised data for research purposes.

5.5 Schedule 2 condition

A Schedule 2 condition must be met when personal data is processed.

Schedule 2 Section 5 (b)[17] permits processing when governing legislation empowers a data controller to carry out a particular function. The NHS Act provides the legal power for an NHS Trust to conduct clinical trials and research therefore this condition is satisfied.

Schedule 2 Section 3 permits processing where it is necessary for compliance with any legal obligation to which the data controller is subject. Personal data about clinical trial participants is being processed in accordance to the Medicines for Human Use (Clinical Trials) Regulations 2004 and Amendment 2006 therefore this condition is also met.

5.6 Schedule 3 condition

In addition to a Schedule 2 condition (above) a Schedule 3 condition should also be met when sensitive personal data is processed. The sensitive personal data categories processed for clinical trials and research will most commonly include the racial or ethnic origin of the data subject and their physical or mental health condition.

[16]http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx

[17] DPA Schedule 2 section 5 (b) for the exercise of any functions conferred on any person by or under any enactment

Schedule 3 Section 8 permits processing when it is necessary for a medical purpose, which includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.[18] Processing confidential personal data is essential for the safe care and management of the individual patient during a clinical trial therefore Schedule 3(8) qualifies. The Information Commissioner's Office has confirmed that Schedule 3(8) is likely to be an applicable condition for the collection and processing of the EDGE patient data set[19].

It should be noted that the Act only requires one condition to be met to legitimise all of the data processing for that specific purpose and the Data Processor organisations are processing the data on behalf of the Data Controller for that purpose.

As part of the recruitment process, clinical trial patients and research participants will have consented to take part in that trial or study. That process should include a fair processing explanation as to how their personal data will be used, which would satisfy the common law requirement for consent. It is, however, the Subscriber Data Controller's responsibility to ensure all legal bases have been met.

5.7 Processing Anonymised data

The Information Commissioner's Anonymisation Code of Practice says:

"*Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. Fewer legal restrictions apply to anonymised data.*" [20]

It goes on further to say (in section 4) that consent is not generally needed to legitimise an anonymisation process, but for processing to be fair consideration has to be given to what people were told when the data was collected for the original purpose and if the intention is to anonymise information then organisations should include this in their privacy notices.

The Code (page 14) provides a summary of the relevant case law R (on the application of the Department of Health) v Information Commissioner [2011] EWHC 1430 (Admin) that establishes the legal precedent for the extraction of anonymised data from medical data.

The Information Standards Board (ISB) standard 1523 Anonymisation Standard for Publishing Health and Social Care Data also provides further information.[21]

---

[18] DPA Schedule 3 section 8 (1) and (2)

[19] http://www.edgeclinicalresearch.com/edge-data-protection/

[20] ICO Anonymisation Code of practice http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx

[21] ISB 1523 Anonymisation Standard for Publishing Health and Social Care Data - http://www.isb.nhs.uk/library/standard/128

The HSCIC guide (Rule 3) provides further information about confidentiality and the application of the Anonymisation standard in health and social care services.

Consent is not necessary to legitimise an anonymisation process, but consideration has to be given to what people are told when their personal data is collected and organisations should inform people that their data will be anonymised and used for research purposes. (See Fair processing 5.4)

5.8 The Seventh DPA principle

The seventh principle of the Act contains certain provisions that apply when a Data Controller contracts a Data Processor to process data on their behalf. In particular, a written contract needs to be in place to set out what the data processor is allowed to do with the personal data and the security measures that the data processor is required to have in place to ensure the protection of that data.

The Subscriber, as the Data Controller, and in order to comply with the seventh DPA principle, must have a written contract with their Data Processor that sets out the required organisational and technical security measures that must be in place to protect the data and instructions for processing.

5.9 The Contract

The Master Services Agreement sets out the contractual terms and conditions for the provision of licences to subscribers and for the implementation and use of the EDGE system. Subscribers are bound to the terms and conditions through a Form of Adherence.

Schedule F of the Master Services Agreement is a Data Controller/Data Processor contract issued in accordance with Schedule 1 part 2 sections 12 (a) and (b) of the DPA (Appendix B).

5.10 Information Security

Schedule F Section 3 of the Data Controller/Data Processor contract sets out the obligations of the Data Processor to establish appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

The organisational, operational and technological processes and procedures adopted are required to comply with the requirements of ISO/IEC 27001:2005 as appropriate to the services being provided to the Data Controller. Where relevant, the Data Controller will use ISO/IEC 27002:2005 as a basis for auditing compliance with the guarantees the Data Processor provides in relation to this obligation.

UOS and Piksel Carelink both ensure that all of their employees who provide the services as defined in the Agreement have undergone information governance training and understand their duty of confidentiality under contract and in the care and handling of Personal Data. This is written into the Master Services Agreement and contract.

EDGE is secure from unauthorised access by the use of a username and password. Users sign on to the application using these credentials. The URL of the sign on page has a HTTPS address to ensure that the HTTPS security protocol is used. Any attempts to open under HTTP will be forced to HTTPS. This results in a layer or security encryption being applied to the session between the client browser and the application within the hosting environment.

The Subscriber organisation is responsible for creating and managing the issue of EDGE passwords to their authorised staff in accordance to the licence agreement and to ensure that they are aware of and comply with the data protection regulations.

It is the Subscriber organisation's responsibility to manage their own access controls for the registration and de-registration of authorised users of the system and to take all practicable steps to prevent unauthorised disclosure and use in accordance with local information governance policies and terms of the Agreement.

5.11 Application Audit

EDGE application has a complete audit of system access and actions; all activities are time date and user stamped.

If UOS has reason to believe that there is likely to be or has been a breach of security or misuse of the System, UOS may change any or all of the end-user passwords and notify the Subscriber accordingly.

The Subscriber organisation should investigate a reported incident and take steps to ensure that any non-compliance issue is addressed in accordance with local information governance policies and Department of Health policy.

Further information about the current process for managing incidents can be found within the latest 'Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation.' [22] [23]

It is the Subscriber organisation's responsibility to investigate any such incident reported to them by UOS in accordance with the Department of Health policy.

5.12 Hosting Arrangements Information Security

UOS has sub-contracted Piksel Carelink[24] to provide the secure managed hosting services platform for EDGE on the N3 network.

Piksel Carelink, as a Data Processor, are required to provide sufficient assurances that their technical and organisational measures adequately protect the personal data they are required to process on behalf of the Data Controller.

Piksel Carelink are the longest established, most highly accredited specialist provider of N3[25] managed hosting services. They have been providing managed hosting on N3 (formerly NHSnet) since 1998.

Information security is assured through:

- ISO 27001[26], ISO 20000, ISO 9000 accreditation, and
- ISO 27001 Tier 4 data centres.

The standard tool used for assessing and assuring an organisation's level of information security is the Health and Social Care Information Centre (HSCIC) Information Governance Toolkit (IGT).

In order to satisfy the NHS Information Governance Statement of Compliance (IGSoC)[27] for the N3 connection, Piksel Carelink complete and submit a satisfactory IGT assessment annually.

---

[22] https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf

[23] IG Serious Incidents Requiring Investigation (SIRI) procedure https://www.igt.hscic.gov.uk/resources/IGIncidentsPublicationStatement.pdf

[24] http://www.carelink.co.uk

[25] http://systems.hscic.gov.uk/n3/factsheet

[26] Information about 27001 and the audit and certification scheme is available at http://www.27001-online.com/

Piksel Carelink's organisation code is 8GX09 and their published submission is available on the IGT webpage https://www.igt.hscic.gov.uk/

Subscriber organisations, as the Data Controller, are required to take reasonable steps to check the Data Processor's security measures are being put into practice to comply with the seventh DPA principle.

UOS undertake the responsibility for ensuring Piksel Carelink's compliance with the terms and conditions of the contract on behalf of the Data Controllers. However, the Data Controller cannot delegate their legal responsibility to UOS and therefore may decide to take their own action to obtain the necessary assurances. In addition to the ISO accreditation and IGT reports that provide evidence of compliance, the Schedule F Data Controller/Data Processor contract provides the right to carry out audit checks to ensure the Data Processor is adhering to the terms of the agreement if the Data Controller considers this to be necessary.

Subscriber organisations are responsible for ensuring their contracted Data Processors comply with the seventh DPA principle and implement effective technical and organisational measures to protect personal data. Piksel Carelink provide evidence of ISO and IGT compliance to UOS who manage the contract on behalf of the Subscriber. Compliance audits can be arranged at the Subscribers discretion. (See Schedule F 2.5)

6 NHS Act Section 251

Section 251 of the NHS Act 2006[28] allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes[29] where:

- The purpose is in the public interest e.g. important medical research and essential NHS activity, and
- It is not possible to use anonymised information for the specified purpose; and
- Where consent has not been obtained to use people's personal confidential data and seeking consent is not practicable.

"Section 251 support" or "Section 251 approvals" refer to approval provided under the Health Service (Control of Patient Information) Regulations 2002.

[27] http://systems.hscic.gov.uk/infogov/igsoc/background

[28] Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006

[29] S.251 (12) NHS Act 2006: In this section "medical purposes" means the purposes of any of—(a) preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services, and (b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment.

Following the enactment of the Health and Social Care Act 2012, the Health Research Authority (HRA) approves medical research applications for s251 support, subject to approval from a research ethics committee. Only the Secretary of State for Health can approve the processing of personal confidential information for any relevant non-research activity under the amended provisions of s251.

The Confidentiality Advisory Committee[30] provides independent expert advice to the HRA and to the Secretary of State for Health regarding whether or not applications should or should not be approved. CAG must advise the Secretary of State on an interpretation and application of the Regulations that is consistent with s.251 NHS Act 2006. Furthermore, regulations made under s.251 may not make provision for processing "in a manner inconsistent with any provision made by or under the Data Protection Act 1998.

For further information see the CAG Principles of Advice – Exploring the concepts of Public Interest' and 'Reasonably Practicable'[31]

6.1 Section 251 in relation to EDGE

Clinicians and nurses conducting clinical trials or research studies are responsible for that they have legitimate grounds for collecting and using personal and sensitive personal data for those purposes.

Section 251 would not apply to clinical trials. Regulations made under S.251 (6)[32] "may not make provision for the processing of confidential patient information solely or principally for the purposes of determining the care and treatment to be given to particular individuals."

There may however be occasions where the clinician or research nurse working for a Subscriber organisation is conducting research under s251 approval and using the EDGE functionality to manage that study.

This is an arrangement between the researcher and CAG, and whist the application process will include an assessment to ensure that appropriate technical and organisational measures are in place, it does not affect or change this guidance. The Subscriber, as the Data Controller is already responsible for ensuring those measures.

Neither is it necessary to obtain s251 approval to support the processing of data within EDGE.

[30] Formerly, the Patient Information Advisory Group (PIAG) (10 December 2001 – 31 December 2008) and the NIGB Ethics and Confidentiality Committee (01 January 2009 – 31 March 2013)
[31] Health Research Authority http://www.hra.nhs.uk/hra-confidentiality-advisory-group/
[32] S.251(6) NHS Act 2006

7 Information Sharing with NIHR CRN

NIHR CRNs are an evolving part of the NIHR. Further information about the NIHR CRN's roles and responsibilities can be found on their webpage[33] however for the purpose of this guidance the NIHR CRN, acting on behalf of their local research groups or other organisations in England with a requirement to report to the NIHR, acquire the right to become Subscribers of the EDGE system, to obtain the services provided by UOS under the terms of the licence Agreement.

Part of that agreement includes the extraction of data generated/held in the system relating to NIHR adopted trials for use in a Central Portfolio Management System (CPMS).

7.1 Anonymised data

The data obtained is anonymous data. Chapter 5.7 explains the legal basis for processing anonymised data and fair processing.

The Subscriber organisation, by signing the Master Services Agreement (section 2) and Form of Adherence are agreeing to allow the data to be extracted.

NIHR CRN, as a publicly funded organisation, will have a mandate to obtain and publish anonymised data for research purposes, but as the data is effectively de-identified the DPA or confidentiality laws do not apply therefore there is no requirement to assign a DPA role or relationship with the identified Data Controllers and Data Processors.

The Subscriber organisation, as the Data Controller and therefore accountable for the data whilst it is held as personal data, are responsible for ensuring that the data extract is effectively anonymised in accordance to the HSCIC Anonymisation Standard (ISB standard 1523).[34]

Assurance that data has been anonymised to the effect that it can be lawfully published and used without breaching confidentiality can only be limited and based on a risk assessment. Subscriber organisations therefore need to agree the minimum data set for the extract to be satisfied that the risk of re-identification is so low that it can be authorised for release.

The HSCIC's Guide to confidentiality provides further information about the necessary controls that are required to protect non-identifiable data where there is a perceived risk of re-identification. This is evolving policy and the HSCIC over time will publish procedures for assessing data collections for publication.

---

[33] http://www.crncc.nihr.ac.uk/homepage

[34] See 20

7.2 Personal confidential data

Clinicians and nurses conducting clinical trials are legally required (in addition to other obligations) to record and provide information in accordance with the Medicines for Human Use (Clinical Trials) Regulations 2004 and Amendment 2006.

In certain limited circumstances, this will include an obligation to report personal confidential data to the NIHR CRN.

It is the responsibility of the clinician or research nurse to ensure the legitimate bases for sharing personal confidential data about their clinical trial (or research) patients with NIHR CRN and to provide that information to them directly as opposed to instructing UOS to report via the EDGE system.

Subscriber organisations when authorising the extraction of data from the EDGE system are responsible for ensuring that the agreed data sets effectively anonymise so that data can be lawfully published and used without breaching confidentiality.

It is the responsibility of the Subscriber organisation's accountable clinician or research nurse to report personal confidential data to NIHR CRN when legally obliged to do so and in accordance with the DPA and confidentiality laws.

8 List of Subscriber responsibilities:

Section	Requirement	Responsibility
2	Research Governance	The NHS organisation subscribing to the EDGE system is responsible for ensuring that the clinical trial and research programmes conducted by their clinicians and nurses conform to the relevant protocols and lawful practice, which in addition to research governance includes information governance.
5.1	DPA Data Controller/Data Processor	The Subscriber is the Data Controller and legally responsible for ensuring that personal confidential data about their respective patients and held within the EDGE system is processed in accordance with the data protection principles. UOS and Piksel Carelink are Data Processors.
5.3	DPA First principle-lawful processing	The NHS Organisation conducting the clinical trial or research study is responsible for ensuring that they have legitimate grounds for collecting and using personal and sensitive personal data and do not do anything unlawful with the data.
5.4	DPA First principle- fair processing	The NHS Organisation conducting the clinical trial or research study is responsible for ensuring that the patients recruited for a clinical trial or research study have been provided with fair processing information (privacy notices) that clearly explains what you intend to do with their personal data, who it will be disclosed to and the intention to use anonymised data for research purposes.
5.7	Processing anonymised data	Consent is not necessary to legitimise an anonymisation process, but consideration has to be given to what people are told when their personal data is collected and organisations should inform people that their data will be anonymised and used for research purposes. (See Fair processing 5.4)
5.8	DPA Seventh principle	The Subscriber, as the Data Controller, and in order to comply with the seventh DPA principle, must have a written contract with their Data Processor that sets out the required organisational and technical security measures that must be in place to protect the data and instructions for processing.

Section	Requirement	Responsibility
5.9	DPA Seventh principle Data Processor/Data Controller contracts	Schedule F of the Master Services Agreement is a Data Controller/Data Processor contract issued in accordance with Schedule 1 part 2 sections 12 (a) and (b) of the DPA (Appendix B).
5.10	DPA Seventh principle – Information Security	It is the Subscriber organisation's responsibility to manage their own access controls for the registration and de-registration of authorised users of the system and to take all practicable steps to prevent unauthorised disclosure and use in accordance with local information governance policies and terms of the Agreement.
5.11	DPA Seventh principle- Information Security	It is the Subscriber organisation's responsibility to investigate any such incident reported to them by UOS in accordance with the Department of Health policy.
5.12	DPA Seventh principle – assurance of data processor compliance	Subscriber organisations are responsible for ensuring their contracted Data Processors comply with the seventh DPA principle and implement effective technical and organisational measures to protect personal data. Piksel Carelink provide evidence of ISO and IGT compliance to UOS who manage the contract on behalf of the Subscriber. Compliance audits can be arranged at the Subscribers discretion. (See Schedule F 2.5)
6.2	Information Sharing Anonymised data	Subscriber organisations when authorising the extraction of data from the EDGE system are responsible for ensuring that the agreed data sets effectively anonymise so that data can be lawfully published and used without breaching confidentiality
6.2	Information Sharing Personal confidential data	It is the responsibility of the Subscriber organisation's accountable clinician or research nurse to report personal confidential data to NIHR CRN when legally obliged to do so and in accordance with the DPA and confidentiality laws.

9 Glossary

Anonymisation:	The process of extracting identifier elements from a data set rendering it into a form where there is little or no risk of re-identification.
Confidential information:	See "Personal confidential data"
Data Controller*:	A person (individual or organisation) who determines the way and the manner in which any personal confidential data are to be processed, including intended to be processed. Data controllers are responsible for ensuring that any processing of personal data for which they are responsible for complies with the data protection principles.
Data Processor*:	In relation to personal data means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
De-identified:	Information from which identities to an individual have been removed, but there is a risk of re-identification.
Identifiable data:	Data that contains an item (identifier), which by itself or in combination with other identifiers enables an individual to be identified. See Appendix B for examples.
Information Governance:	The standards that ensure health and social care services handle information legally, securely, efficiently, effectively.
Personal confidential data:	Personal information about individuals that should be kept private or secret. It is a new term to describe data that includes the DPA definition of personal data and sensitive personal data, but includes information about dead as well as living individuals; and any information given in confidence and/or that which is owed a duty of confidence. It is abbreviated to PCD.
Personal data*:	Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of or likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of intentions of the data controller or any other person in respect to the individual.

Processing*:	Processing in relation to personal data or information mans obtaining, recording or holding the information of data or carrying out any operation or set of operations on the data including: o Organisation, adaption or alteration of the information or data; o Retrieval, consultation or use of the information or data; o Disclosure of the information or data by transmission, dissemination or otherwise making available; or o Alignment, combination, blocking erasure or destruction of the information or data.
Pseudonymisation:	Individuals are distinguished in a data set by removing identifiable data elements and replacing them with a code to provide a unique identifier that does not reveal their "real world" identity.
Re-identification;	Processing, analysing or combining data with other data with the result that individuals become identifiable.
Sensitive personal data*:	Personal data that includes information about the racial or ethnic origin, political opinion, religious belief or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions and legal proceedings against the individual or allegations of offences committed by the individual.

* Data Protection Act 1998 terminology defined in section 1(1)

Appendix A:

MASTER SERVICES AGREEMENT

SCHEDULE F –DATA CONTROLLER AND DATA PROCESSOR CONTRACT

(A) This contract is issued under Schedule 1 part 2 sections 12 (a) and (b) of the Data Protection Act 1998

(B) Each of the Subscribers party to the Master Services Agreement is a Data Controller, in respect of its own Personal Data, and each Data Controller wishes to appoint UOS as their Data Processor for the purpose of enabling the Services as described in the Agreement.

(C) In order to perform the Services on the Data Controller(s)'s behalf, the Data Processor will require certain Personal Data to be made available to it by each Data Controller.

(D) The Data Controller is legally responsible for ensuring all personal data processed under their control is processed in compliance with the eight Data Protection Act principles.

(E) Under the Data Protection Act 1998, each Data Controller(s) is required to put it place a contract between the Data Controller and any organisation which processes Personal Data on its behalf governing the processing of that personal data.

(F) This contract neither replaces nor undermines the terms and conditions set out in the Master Services Agreement but is supplementary to it and binds the parties into a legally enforceable contract under which the Data Processor must act only upon the instruction of the Data Controller

(G) Each of the parties to each individual Licence under the Agreement now describe the terms and conditions of a Data Processor Contract in this Schedule F in order to regulate the processing of Personal Data that the Data Processor will be processing on behalf of each Data Controller.

CONTRACT

DEFINITIONS AND INTERPRETATION

In this Data Processor Contract:
The following have the same meaning as defined in section (1) and section (2) of the Data Protection Act 1998, but for the purpose of this contract:

Data Controller:	means the respective Subscriber who is party to that Subscription and Services Agreement
Data Processor:	means the University of Southampton or UOS and Piksel Carelink
Data Processing:	means obtaining, recording or holding information or data or carrying out any operation or set of operations on the data etc.
Data Subject:	Means an individual who is the subject of Personal Data;
Personal Data:	Means data which relate to a living individual who can be identified from that data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller or data processor etc.
Sensitive Personal Data:	Means personal data consisting of information as to the racial or ethnic origin of the data subject, his physical or mental health condition, or other sensitive data specified in the Act section (2).

1.1 This Agreement shall continue in full force and effect for the same period unless terminated by either party.

2. **OBLIGATIONS OF A DATA CONTROLLER**

2.1 Each Data Controller is, in accordance with Section 4(4) of the Act, legally responsible to ensure compliance with the data protection principles in relation to all personal data with respect to which they are the data controller.

2.2 Each Data Controller is responsible for ensuring the Personal Data processed for the purposes of this Agreement has been obtained in accordance with the Act and relevant legislation.

2.3 Each Data Controller shall provide the Personal Data to the Data Processor together with such other information as the Data Processor may reasonably require in order for the Data Processor to provide the Services.

2.4 The instructions given by each Data Controller to the Data Processor in respect of the Personal Data shall at all times be in accordance with relevant legislation.

2.5 The Data Controller reserves the right upon giving reasonable notice and within normal business hours to carry out compliance and information security audits of the data processor in order to satisfy itself that the Data Processor is adhering to the terms of this agreement.

3. OBLIGATIONS OF THE DATA PROCESSOR

3.1 The Data Processor undertakes that it shall process the Personal Data strictly in accordance with each Data Controller's instructions for the processing of the respective Personal Data.

3.2 The Data Processor will process the Personal Data exclusively for the purpose of supplying the Services in Local Portfolio Management System for clinical research or clinical trials being managed by a Subscriber(s).

3.3 The Data Processor will treat the Personal Data, and any other information provided by a Data Controller as confidential.

3.4 The Data Processor will process the Personal Data in compliance with the Data Protection Act 1998.

3.5 The Data Processor agrees to provide each relevant Data Controller promptly with all subject information requests which may be received from the Data Subjects of the Personal Data;

3.6 The Data Processor will take reasonable steps to ensure the reliability of any employees who have access to personal data and will ensure that only such of its employees who may be required by it to assist it in meeting its obligations under the Agreement shall have access to the Personal Data.

3.7 The Data Processor will ensure that all employees used by it to provide the Services as defined in the Agreement have undergone training in the law of data protection, their duty of confidentiality under contract and in the care and handling of Personal Data.

3.8 The Data Processor will:

3.8.1 subject to clause 3.8.3, not disclose the Personal Data to a third party in any circumstances other than at the specific written request of the relevant Data Controller, unless the disclosure is required by law; and

3.8.2 inform the Data Controller of any request or instruction to disclose Personal Data as required by law where that request or instruction has not originated from the Data Controller.

3.8.3 Allow the National Institute for Health Research, or its successor organisation(s), to access and collate Personal Data, exclusively within a Central Portfolio Management System, subject to such use being authorised by the Data Controller and in accordance with UK Data Protection law and regulations.

3.9 The Data Processor will NOT transfer the Personal Data outside of the European Union.

3.10 The Data Processor has sub-contracted Piksel Carelink to provide the secure managed hosting services platform for EDHE on the N3 network, but will not further sub-contract any of the processing without explicit written agreement from the relevant Data Controller.

3.11 The Data Processor agrees that, where it is permitted to sub-contract, it will ensure on behalf of the Data Controller that any sub-contractor it uses to process the Personal Data complies with the 7th Data Protection Act principle and terms of this Contract.

3.12 The Data Processor agrees that a Data Controller may, upon giving reasonable notice and within normal business hours, carry out compliance and information security audits and checks of the sub-contractor to ensure adherence to the terms of this Agreement.

3.13 The Data Processor will employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure. The organisational, operational and technological processes and procedures adopted are required to comply with the requirements of ISO/IEC 27001:2005 as appropriate to the services being provided to the Data Controller. Where relevant, the Data Controller will use ISO/IEC 27002:2005 as a basis for auditing compliance with the guarantees the Data Processor provides in relation to this obligation.

3.14 The Data Processor will not keep the Personal Data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use

of the device or laptop is necessary for the provision of the Services under this Agreement. Where this is necessary, the Data Processor will keep an audit trail of which laptops/drives/devices the Personal Data are held on.

3.15 On satisfactory completion of the Services or on termination of this Agreement, the Data Processor will ensure that the relevant Personal Data is securely removed from their systems and any printed copies securely destroyed. In complying with this clause, electronic copies of the Personal Data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets HM Government standards. Any hard copy will be destroyed by cross-cut shredding or subcontracted to a confidential waste company that complies with European Standard EN15713 and assures secure re-cycling of the resulting paper waste.

3.16 On being informed by a Data Controller of the death of a Data Subject the Data Processor will ensure that the relevant Personal Data relating to that Data Subject is securely removed from their systems and any printed copies securely destroyed in accordance with the relevant Data Controller's records retention policy.

3.17 The rights, obligations and benefits of the Data Processor (UOS) in respect of this Data Processor Contract may be assigned or otherwise transferred to any person who acquires substantially all of the UOS's assets used in its business relating to this Data Processor Agreement or to any other person, with the prior written consent of the relevant Data Controller, which shall not be unreasonably withheld.

4. THIRD PARTY RIGHTS

4.1 Any Data Subject is hereby entitled to enforce the terms and conditions of this Data Processor Agreement as a third party beneficiary.

5. FREEDOM OF INFORMATION

5.1 ANY INFORMATION PROVIDED to the Data Processor by a Data Controller, shall be deemed to be 'held' on behalf of the relevant Data Controller and as such the Data Processor will:

5.1.1 **TRANSFER** any requests seeking access to any part of that information which fall within the provisions of the Freedom of Information Act 2000 to the relevant Data Controller as soon as is reasonably practical, who will then be responsible for processing the request; and

5.1.2 **PROVIDE** all reasonable assistance to enable the relevant Data Controller to fulfil their legal obligations in respect of any freedom of information requests.

6. INDEMNITIES

6.1 The Data Processor shall indemnify the relevant Data Controller against any breach of the Act or any other statutory obligation committed by the Data Processor which renders the Data Controller liable for any costs, fines, claims or expenses, (including reasonable legal fees and disbursements) however arising, including, but not limited to any deliberate or reckless acts or omissions of the Data processor employees.

7. GOVERNING LAW

7.1 This Agreement shall be governed by and construed in accordance with English law and each party hereby submits to the exclusive jurisdiction of the English courts.

8 SERIOUS INFORMATION BREACH INCIDENT, INCIDENT REPORTING AND DUTY OF CANDOUR.

8.1 The Data Processor shall have procedures in place to record and report any actual or suspected misuse of authorised access rights.

1.1 8.2 If UOS has reason to believe that there is likely to be or has been a breach of security or misuse of the System, UOS may change any or all of the End-User passwords and notify the Subscriber accordingly.

8.3 In so far as the Data Controller is responsible for the personal data, it is the Data Controller's responsibility to ensure that the actual or suspected incident is investigated, reported in accordance with the Department of Health policy and procedures and for informing the relevant data subjects as appropriate.

Appendix B

List of Identifiable data items

The following list is derived from the HSCIC Guide to Confidentiality – References document http://www.hscic.gov.uk/confguideorg

An identifier is an item of data, which by itself or in combination with other identifiers enables an individual to be identified. Examples include:

1. Names
2. All geographic subdivisions smaller than a state[35], including street address, city, county, precinct, postcode, and their equivalent geographical codes, except for the first four digits of a postcode if, according to the current publicly available data from the Office for National Statistics and/or the Information Commissioner's Office:
    a) The geographic unit formed by combining all postcodes with the same four initial digits contains more than 20,000 people.
    b) The initial three digits of a post code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such an age, except that such ages and elements maybe aggregated into a single category of age 90 or over.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. National Insurance numbers.
8. NHS number and medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/licence numbers.
12. Vehicle identifiers and serial numbers including licence plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) addresses numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.

[35] This list was adapted from those published as part of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The HIPAA Privacy Rule is the first comprehensive federal protection for the privacy of personal health information. More information is available at the website: http://privacyruleandresearch.nih.gov/pr_08.asp

18. Any other unique identifying number, characteristic or code, unless otherwise permitted by the Information Commissioner's office.

The HSCIC Anonymisation standard (ISB 1523 Anonymisation Standard for Publishing Health and Social Care Data) http://www.isb.nhs.uk/library/standard/128

The Information Commissioner Anonymisation Code of Practice: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx