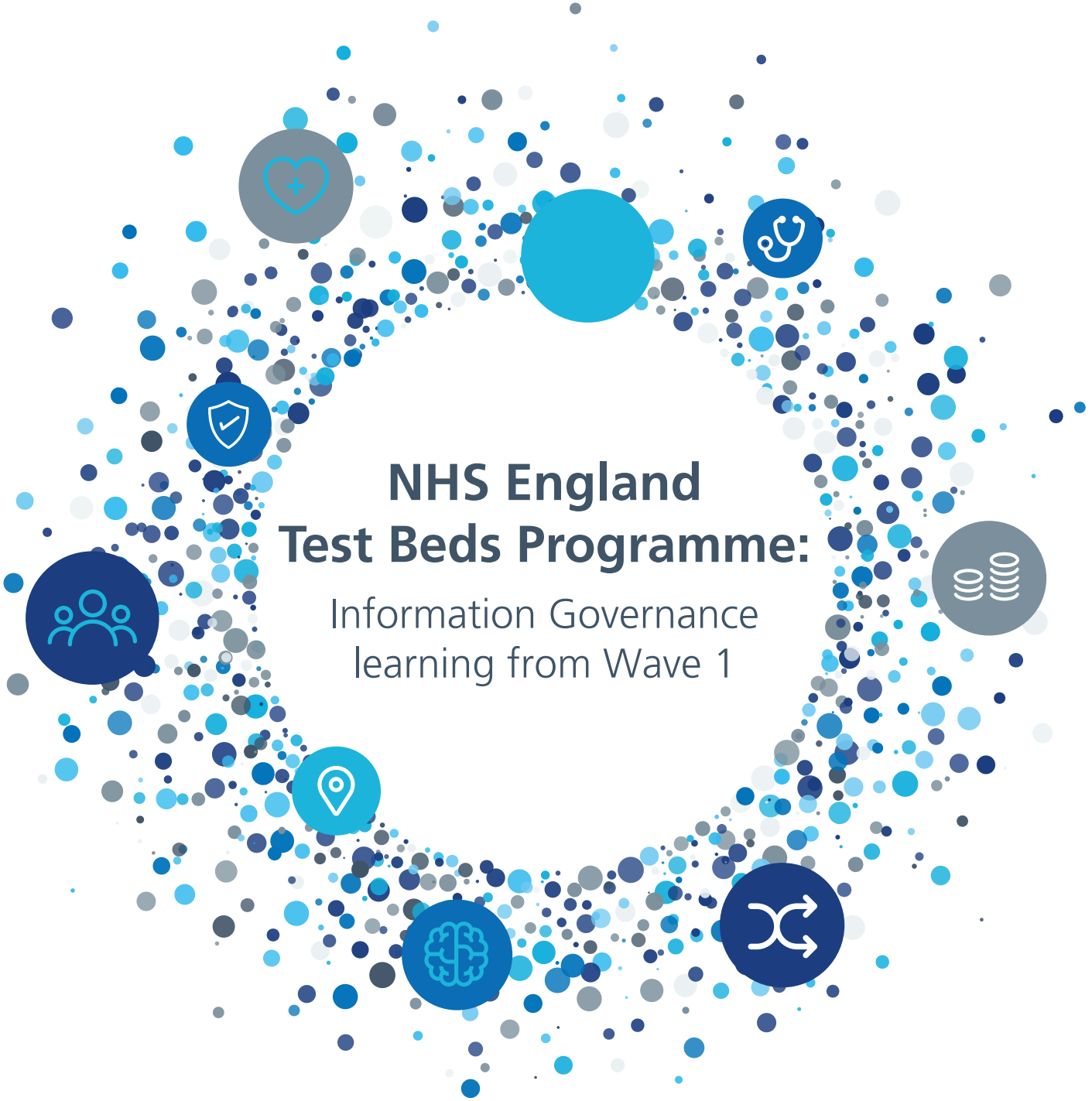
NHS England



NHS England Test Beds Programme:

Information Governance learning from Wave 1

Contents


Section 01

Introduction

The Test Beds programme: harnessing technology, transforming care

The Test Beds programme is funded by NHS England, the Department of Health and the Office for Life Sciences. It is a pioneering project which combines digital technologies and new models of care and tests them in real world settings. The programme aims to generate evidence that can drive the uptake of digital innovations at scale and pace across the health and care system and share learning around what works. Its primary objective is to harness the potential of digital technologies in the provision of care and improve the quality of life for patients and carers. This includes supporting self-management, early diagnosis, preventing unnecessary hospital admissions and bringing care closer to home.

Another key feature of the Test Beds programme is collaboration. Each Test Bed brings together partners from across the NHS, academia, industry and patient groups. They are working in partnership to improve patient outcomes and deliver care at the same or less cost. This handbook brings together the wealth of knowledge generated from Wave 1 of the programme and includes learning recommendations and reflections on information governance. It forms part of a suite of Test Beds legacy and learning publications that seek to share learning from the programme with both future Test Beds and the wider health and care system.

The importance of information governance to the Test Beds programme

Information governance is a key enabler which supports effective sharing and management of information in the NHS. Establishing and maintaining information governance arrangements is a crucial part of the set-up and successful operation of Test Beds. Sites are required to understand their information governance requirements, including the use of personal and sensitive information relating to patients and employees. They will need to undertake relevant activities to ensure that they are compliant with national legislation, for example, the General Data Protection Regulation. Information governance issues underpin and affect multiple aspects of Test Beds including governance arrangements and collaborative working with industry.

About this handbook

This Information governance handbook is designed to support a future wave of Test Bed programme leaders, project managers and information governance staff to:

- understand common information governance challenges faced by the initial Wave 1 Test Beds and benefit from their learning
- plan similar information governance activity and access tools and guidance that can support their work.

The document also aims to share learning from the programme with both future Test Beds and the wider health and care system.

It is designed to support information governance leadership at all levels within Test Beds and includes tailored content for programme leaders, project managers and information governance staff who have varying levels of information governance knowledge. It also features information and tools that can help different team members to understand the information governance considerations for their projects, identify and manage information risks and learn about key principles and enablers that can help their work to succeed.

This handbook is structured in three parts:

- **Section 2** includes information on the technologies used by Wave 1 Test Beds (such as apps and algorithms) and helpful lessons learned
- **Section 3** describes information governance tools and enablers that can be used by a future wave of Test Beds to support their work (e.g. data flow mapping)
- **Section 4** shares key issues for consideration for a future wave of Test Beds programme/ project managers and information governance leads and includes advice on what these different audiences need to do

It is designed to be an active tool which a future wave of Test Bed staff can 'dip into' throughout the course of the programme and support programme set-up. It is accompanied by a checklist, which is a reminder for a future wave of Test Beds regarding what they need to do on information governance, and a supporting annex which has a list of useful links.

The Test Bed sites and technologies trialled

The map below sets out the technologies trialled at each Test Bed site. All sites tested at least two types of technological intervention in real world settings and with the aim of tackling a wide range of conditions. Detailed descriptions of each technology are provided opposite.

1 Lancashire and Cumbria Innovation Alliance

Improving support for those over 55 with Chronic Obstructive Pulmonary Disease, heart failure and dementia. Integrating technologies and linking them to new care models supporting self-care at home.

D E F H I

2 Long Term Conditions Early Intervention Programme

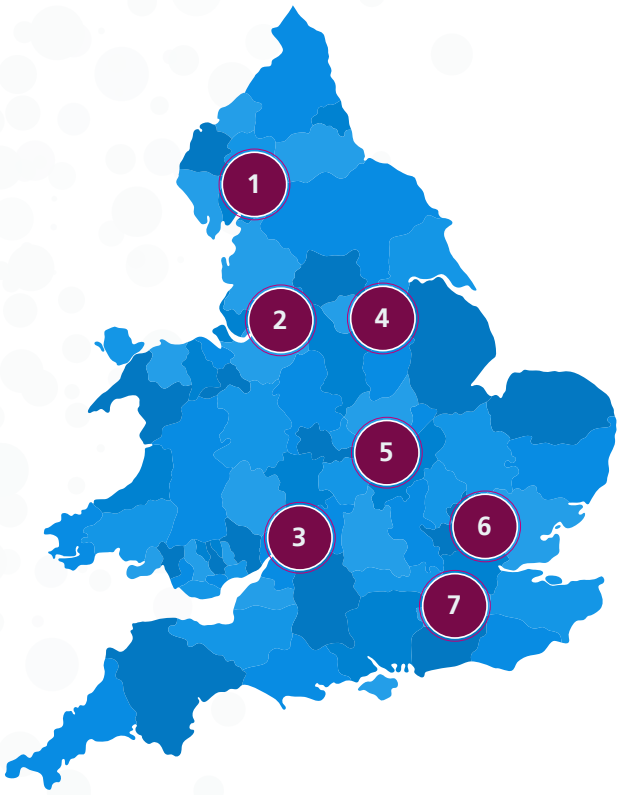
Improving the ability to detect, manage and prevent long-term ill health by using pseudonymised data and telecare technology.

A B

3 Diabetes Digital Coach

Facilitating improved self-management of diabetes through the use of integrated digital tools, including the use of Internet of Things technology.

E H D



4 Perfect Patient Pathway

Improving pathways for asthma, diabetes, falls and frailty by increasing access to technology and facilitating information sharing.

B D F H

5 RAIDPlus

Developing a demand and capacity tool that shows patient flow in real-time and a predictive algorithm to identify when people are going to experience a mental health crisis.

A B

6 Care City

Testing a combination of digital devices and software alongside new approaches to service delivery and patient participation. Example conditions include dementia and falls and frailty related injury.

D E G H I

7 Technology Integrated Health Management

Providing people with dementia and their carers with: wearables, monitors and other devices which will combine into an 'Internet of Things' to monitor their health at home.

D E

A

Risk Stratification for Case Finding

Risk stratification for case finding utilises known markers in the patient record that suggest the likelihood of a particular outcome for a patient, based on a number of patient attributes. An algorithm is generally used to generate a "risk score" for each patient.

B

Algorithm Development

The development of an algorithm requires large volumes of historic patient data where the outcome for the patients is known so that, from a common known outcome, it is possible to track back in the health record and identify common early indicators that may have contributed to that outcome.

C

Data Analytics and Dashboarding

In this context, the terms Data Analytics and Dashboarding refer to the production of a live feed of data which populates a dynamic dashboard to enable near to real-time response times to changes in circumstance.

D

Patient Held Devices & Apps

Devices or applications (in some cases the applications are classed as devices), through which the patient interacts and provides information to be used in monitoring their care requirements.

E

Internet of Things

Internet of Things in this context refers to the use of sensors such as wearables, monitors and other devices to monitor health in the home, enabling patients to take greater control of their health and well-being.

F

Technology Enabled Delivery

This term is used to describe interventions where technology is being used to transform care interactions. Examples from Wave 1 Test Beds include the use of video consultations and online communities to support those with long term health conditions.

G

Technology Enabled Research and Evaluation

The use of patient data to support research. This often involves seeking consent from individuals to use their data for research purposes, a process described as "Consent to Contact".

H

Devices and Apps for Professionals

Devices and apps for professionals allow staff to deliver care in a technology enabled way and in the case of the Test Beds sites, typically enabled professionals to operate more flexibly, for example through the use of portable gait assessment devices.

I

Technology Enabled Social Prescribing

Social prescribing, sometimes referred to as community referral, is a means of enabling GPs, nurses and other primary care professionals to refer people to a range of local, non-clinical services. Social prescribing schemes can involve a variety of activities which are typically provided by voluntary and community sector organisations. Examples include volunteering, arts activities, group learning, gardening, befriending, cookery, healthy eating advice and a range of sports.

Planning an effective approach to information governance

Information governance resources must be involved and empowered from the outset of projects. Based on Wave 1 experience, it is vital to plan for, and address, information governance risks through the life of a project – from inception, during the set-up phase, to the conclusion of operations and wrapping up. The diagram below outlines some of the key activity required at each stage of a project, for both non-technical and more specialist roles. More detailed advice and guidance is included in this handbook.

Programme or Project Manager

PROJECT SETUP

- Review project lifecycle for key IG touchpoints and milestones
- Undertake initial assessment and estimate of required information governance resources
- Engage IG teams to co-develop resourcing plan
- Agree ways of working with IG teams, specifically the trigger points for engagement and how they are empowered through project governance
- Evaluate Technology Partner information governance capability

MONTHS 0-1

MAPPING DATA

MONTHS 1-2

- Outline and agree comprehensive overview of project stakeholders and associated roles and responsibilities
- Review and understand the key IG challenges posed by proposed governance structures
- Produce project documentation on the results of data asset and flow mapping activities

IDENTIFYING RISKS

MONTHS 2-3

- Agree plan for aligning IG resource to complete Data Protection Impact Assessment (DPIA)
- Disseminate key findings of DPIA to relevant stakeholders
- Review and add key project risks (from DPIA) into overall risk log and reflect actions and reviews into project plan
- Review DPIA(s) quarterly with senior stakeholders

MANAGING RISKS

MONTHS 3-15

- Regularly review risk log for new risks, progress or remedial activities and changes to impact and likelihood
- Document and address the impact of IG risks on other project workstreams
- Ensure alignment of IG resource for completion of risk mitigation activities
- Carry out monitoring, adjustments and reporting on risks as the project evolves
- Conduct monthly risk review meeting

PROJECT CLOSE DOWN

MONTHS 15-18

- Incorporate IG compliance into planning for project close down activities
- Review key documentation and account for identified actions
- Populate and complete document repository for confirmation of data deletion or retention

Information governance Lead

PROJECT SETUP

- Engage project team to gain an understanding of project structure and deployed technologies
- Review and agree IG milestones and match expertise and capacity to needs
- Produce high level report on IG risks created as a result of project structure, in terms of governance accountability and partner relationships
- Implement standing item for IG at project governance meetings
- Evaluate Technology Partner IG capability

MONTHS 0-1

MAPPING DATA

MONTHS 1-2

- Undertake detailed mapping exercise of proposed data flows
- Define the key roles and responsibilities of stakeholders, including controller/ processor relationships
- Undertake mapping exercise of formal contractual relationships between parties

IDENTIFYING RISKS

MONTHS 2-3

- Undertake completion of the DPIA to identify associated IG risks
- Develop and record appropriate, post-DPIA mitigatory actions and controls
- Agree cross partnership support for the findings of the DPIA and create time-limited actions for remedial activity
- Review DPIA(s) quarterly with senior stakeholders

MANAGING RISKS

MONTHS 3-15

- Support in undertaking and reviewing remedial action for identified risks
- Regular evaluation of ongoing IG risks and review of the DPIA
- If proportional to identified risk, arrange and carry out spot checking and control validation exercises
- Conduct monthly risk review meeting

PROJECT CLOSE DOWN

MONTHS 15-18

- Identify, plan and communicate IG close down activities to stakeholders
- Provide specialist advice on ongoing processing activities and support evidencing of winding up procedures and data retention

Section 02

Test Bed technologies: Lessons learned

Sites participating in Wave 1 of the Test Beds programme piloted a number of different technologies in real world settings. Each technology presents a specific set of information governance implications and related requirements. This section describes the key lessons learned and offers advice for future Test Bed sites.

Risk stratification for case finding

Context

The **RAIDPlus** and **Long Term Conditions Early Intervention Programme Test Beds** sought to use risk stratification to identify opportunities for more targeted support. The ultimate aim of these Test Beds was to drive a more prevention focused set of interventions – rather than the reactive approaches typically seen across the system.

- **Case finding** is a process to actively identify individuals from a larger population for a specific purpose, such as flu vaccination
- **Risk stratification** involves dividing a population into different levels of risk for a specified outcome; for instance, unscheduled admission to hospital.

Risk stratification for case finding combines these to enable health professionals to identify individuals and groups of people who may benefit from targeted inventions. Risk stratification for population analysis ('population segmentation') groups the local population by the kind of care they need; it may include how often they might need care.

The benefit of this approach is that it can prevent more costly and reactive interventions; for instance, flu vaccinations reducing the risk of hospitalisation.

The current legal basis for the use of identifiable information for population segmentation and risk stratification is Section 251 of the NHS Act 2006.

What are the information governance implications?

The use of patient data for risk stratification and case finding raises a number of information governance challenges. **The Long Term Conditions Early Intervention Test Bed** sought to use risk stratification to inform their early intervention activity. Experience with this site showed that for a project to be successful, it is important that the following issues are taken into account at an early stage:

- patient consent provided for direct care may not be relied on to meet confidentiality obligations for risk stratification: not everyone will be offered further services as a result of their data being processed, and risk stratification is not necessarily a use of their information that people would expect
- Early and transparent communication of your Test Bed's approach to using patient data including benefits and outcomes have to be planned and delivered early, incrementally, and transparently
- sites need to be clear on the purpose of processing and the related legal grounds under the EU General Data Protection Regulation, the common law duty of confidentiality and the Human Rights Act 1998
- when mapping data flows, it is important to identify anonymous and pseudonymous or identifiable data.

Risk stratification for case finding (continued)

What are the information governance implications? (continued)

- robust security controls are needed to prevent any unauthorised interference with the systems in use and to protect data from corruption or unauthorised alteration
- records of due diligence need to be kept in relation to the supplier
- contracts must clearly set out data controller and data processor roles
- the extent of automated processing and profiling should be determined, identifying any applicable rights
- fair processing and privacy notices must include information to be provided to patients where data has been obtained from third parties (General Data Protection Regulation Article 14 – see glossary).

Lessons learned from wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ understand the difference between risk stratification for case finding as opposed to risk stratification for population analysis and the differing implications for data protection approaches – definitions of which can be found in the glossary
- ✓ ensure solution designs for risk stratification for case finding give particular attention to the differences between confidentiality and privacy. These concepts are described in this document's glossary
- ✓ if relying on the national section 251 exemption for risk stratification, ensure compliance with key requirements, see Health Research Authority CAG Guidance link below
- ✓ consider the role of communications and transparency in enabling protection of the data subject's rights and freedoms.

Should not:

- ✓ overlook the requirement under General Data Protection Regulation to undertake public consultation with representative samples of data subjects to inform design of effective messages and test their effectiveness.

Useful Links

NHS England:
Risk stratification

NHS England:
"Using case finding and risk stratification: A key service component for personalised care and support planning" (January 2015)

NHS England:
"Next Steps for Risk Stratification in the NHS" (2015)

Better Care Fund:
'How to' guide: the BCF technical toolkit section 1: Population segmentation, risk stratification & information governance (August 2014)

What needs to be done?

- ✓ complete data flow mapping noting the type of data for each flow (anonymous or pseudonymous)
- ✓ create and deliver an incremental, transparent plan for patient communications as early as possible in the programme
- ✓ complete the Data Protection Impact Assessment
- ✓ clarify who the data controllers are and the lines of accountability
- ✓ carry out supplier due diligence and put in place robust contractual arrangements
- ✓ determine the legal basis for processing
- ✓ if relying on Section 251, ensure the project's plan and design take into account the scheduled expiry of current Confidentiality Advisory Group (CAG) support
- ✓ apply for the required Secondary Use Service (SUS) data flows from NHS Digital
- ✓ ensure systems and processes are in place to manage patient objections and to implement applicable patient rights, including rights linked to automated processing and profiling
- ✓ complete the communications programme, outlined in the corresponding information governance enabler section of this document
- ✓ maintain a watching brief on national policy regarding the continuation of Section 251 support.

National Data Guardian for Health and Care: "Review of Data Security, Consent and Opt-Outs" (June 2016)

NHS Digital: Independent Group Advising on the Release of Data (IGARD) [website]

NHS England: "Fair Processing for Risk Stratification Checklist"

Health Research Authority CAG Applicant Guidance

Algorithm development

Context

The **RAIDPlus**, **Technology Integrated Health Management** and **Long Term Conditions Early Interventions Test Beds** sought to utilise the development of algorithms or machine learning to drive a predictive model of care planning – identifying needs early and tailoring support so as to better target resources and maintain a more independent lifestyle across issues such as mental health, dementia and diabetes.

Artificial Intelligence (AI) is the use of algorithms and software to approximate or exceed the accuracy and speed of human decision making; for instance, in the analysis of complex medical data. AI systems have been used to select the correct customised treatment path based on an analysis of notes from a patient's file, external research and clinical expertise.

Machine learning is a dynamic and progressive process using algorithms to enable computers to improve the speed and accuracy of their decision making, developing their learning over time through data and information from real-world interactions. For example, machine learning is used to 'train' computers to analyse images for diagnostic purposes. By analysing multiple images, the computer learns which features tend to be associated with specific conditions. The more images the computer analyses, the more accurate its predictions should become.

The terms "artificial intelligence" and "machine learning" are not interchangeable so it is important to be clear which of these your Test Bed is deploying. Some applications are likely to require approval from the Medicines & Healthcare products Regulatory Agency.

What are the information governance implications?

The application of AI or machine learning may result in automated processing within the scope of Article 22 of the EU General Data Protection Regulation – see glossary.

It may be unclear whether the organisation developing the AI is a processor or controller, depending on the extent to which the designer of the algorithm determines the manner and purpose of processing or makes decisions affecting the individual.

Useful Links

Medicines and Healthcare products Regulatory Authority

Information Commissioner's Office: "Big data, artificial intelligence, machine learning and data protection" (2017)

Information Commissioner's Office: "Royal Free London NHS Foundation Trust" (July 2017)

Lessons learned from Wave 1 of the Test Beds programme

Although Test Beds project are first and foremost thought of as technology innovation partnerships, they are almost all also health research projects that may involve the creation of medical devices, especially if your programme is developing apps or algorithms. Each site will need to seek expertise and assess its position as a health research and/or medical device programme as each requires additional and lengthy regulatory activity outside of information governance. Experience with the RAIDPlus site in Wave 1 showed that early assessment against Health Research Authority and Medicines and Healthcare Products Regulatory Agency criteria is a key element of the critical path for Test Bed projects. If the project classifies as research and/or as a device, sites should consider the following:

A) Ensuring a mature hypothesis and testing method is agreed

B) Scheduling early and documented clinical engagement and decisions about what interventions will specifically be trialled

C) Planning for a heavier path of compliance due diligence adding a new 6-12 month compliance activity

D) Monitoring whether regulation may change in the middle of your compliance process and the impact that could potentially have in changing the device classification

E) Budgeting the additional cost to engage a new regulatory process.

Other learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ appreciate that algorithms can be a medical device, and that medical devices should be developed using a structured process from the outset – outlined in the corresponding section of this document
- ✓ acknowledge that certain medical devices may require Medicines and Healthcare Products Regulatory Agency approval.

Should not:

- ✓ underestimate the importance of taking a structured approach to algorithm development from the outset.

What needs to be done?

This is a complex and rapidly evolving area requiring specialist expertise across information governance, algorithm development and a detailed understanding of the objectives of the project. To be prepared, you should:

- ✓ complete data flow mapping
- ✓ understand and plan for your other regulatory compliance requirements around health research (Health Research Authority) and medical device development (Medicines and Healthcare Products Regulatory Agency)
- ✓ complete required Data Protection Impact Assessment(s)
- ✓ carry out supplier due diligence
- ✓ identify and define data controller and processor relationships
- ✓ implement data protection by design and by default
- ✓ complete the communications programme, outlined in the information governance enablers section of this document
- ✓ maintain a watching brief for new developments.

Data analytics and dashboards

Context

The healthcare sector needs interactive performance management tools such as performance dashboards and data analytics to measure, monitor and manage performance more effectively. The level of oversight can vary between organisational, departmental and service level information. It may use real-time (live) or snapshot (point in time) data to inform planning and decision making.

Although all data for publication should be fully anonymised, it is sometimes necessary to use de-identified or pseudonymised granular data for effective internal management and review.

What are the information governance implications?

When developing dashboards or conducting data analysis, it is important to understand the differences between confidentiality and privacy, and between anonymous and personal identifiable data – these terms are clearly outlined in this document's glossary.

The common law duty of confidentiality is only breached if a human sees the data. Although most health-related processing is lawful under EU General Data Protection Regulation Article 9(2)(h) – see glossary, processing must still be fair and transparent – even if there is no human access to identifiable data.

Useful Links

Information Commissioner's Office:
Principle (c): Data minimisation

Information Commissioner's Office: Anonymisation:
managing data protection risk code of practice

Digital: Data and cyber security:
protecting information and data in health and care

Lessons learned from Wave 1 of the Test Beds programme

Although none of the Wave 1 sites ultimately produced dashboards to support clinical decision making, early plans to leverage this technology for the Perfect Patient Pathway Test Bed did provide some learning, suggesting that future projects

Should:

- ✓ understand the difference between privacy and confidentiality, defined in this document's glossary
- ✓ ensure that legitimate relationship controls are embedded such that confidentiality is maintained – aligning closely with the policies of privacy by design and default
- ✓ make sure that data linkage is an expected use of data and that transparency duties have been met.

Should not:

- ✓ miss the opportunity to utilise privacy enhancing technologies to ensure that lawful data processing under privacy law is not confused with the common law duty of confidentiality
- ✓ permit excessive data to be viewed by any single user unless justified by their purpose.

What needs to be done?

To make full use of interactive performance management tools, you need to:

- ✓ complete data flow mapping, noting data controller and processor relationships and any secondary use of the data
- ✓ complete required Data Protection Impact Assessment(s)
- ✓ carry out supplier due diligence
- ✓ ensure adequate safeguards are in place to guard against unauthorised access or unintentional publication or disclosure of personal data sets
- ✓ develop the system following principles of data protection by design and/or by default; for example, by employing data minimisation techniques (defined in the glossary)
- ✓ complete an incremental transparent communications programme.

National Data Guardian for Health and Care: "Information: To Share Or Not To Share? The Information Governance Review" (2013)

National Data Guardian for Health and Care: "Review of Data Security, Consent and Opt-Outs" (June 2016)

Patient held devices and apps

Context

As the wider programme was an exploration of technology driven innovations, a large number of Test Beds looked to exploit data through direct engagement with patient devices. The aims of these Test Beds were mixed, typically aiming to support self-management of conditions. They looked to do so through methods such as informing or refining analytical algorithms to improve case management **(Technology Integrated Health Management and RAIDPlus);** or to better share data with partners to allow for a more collaborative and holistic method of care **(Care City, Perfect Patient Pathway, Diabetes Digital Coach and Lancashire and Cumbria Innovation Alliance)**.

Apps that are classed as medical devices require Medicines & Healthcare products Regulatory Agency (MHRA) approval. A number of sites including, **Care City, Lancashire and Cumbria Innovation Alliance and Technology Integrated Health Management** were required to determine whether their devices met this classification.

A 'medical device' is defined in Article 1 of Council Directive 93/42/EEC and in UK law under The Medical Device Regulations 2002 (Statutory Instrument Number 618) as: 'an instrument, apparatus, appliance, material or other article, whether used alone or in combination, together with any software necessary for its proper application, which –

1. Is intended by the manufacturer to be used for human beings for the purpose of:
   i. Diagnosis, prevention, monitoring, treatment or alleviation of disease
   ii. Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap
   iii. Investigation, replacement or modification of the anatomy or of a physiological process, or control of conception.
2. Does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means.

Medical Device Regulations are changing in the UK from May 2020.

Test Beds will need to plan for this change as it introduces changes such as more complexity around device classification, a rigorous quality management process, and new rules for software development.

What are the information governance implications?

Many of the risks associated with apps arise from the variety of data and sensors held in mobile devices and the extended possibility of tracking the users, especially as people tend to keep smart devices switched on. Users must understand what the app will do with any data they provide.

If the app or device provider is the data controller, explicit consent is needed for the lawful processing for health and care purposes under General Data Protection Regulation Article 9 – see glossary. This is a very high standard to reach as gaining remote consent makes it harder to prove that the subject has made an informed decision.

In addition, use of applications and devices, particularly where the public body is not the Data Controller, can introduce risks to the rights of the data subject. The General

Useful Links

MHRA guidance 2020

European Union: "Privacy Code of Conduct on mobile health apps"

What are the information governance implications? continued

Data Protection Regulation (GDPR) introduces new or enhanced rights for data subjects, including the right to erasure (Article 17), portability (Article 20 – see glossary) and tightened arrangements for compliance with Subject Access Requests (SARs). These risks should be captured and addressed in the Data Protection Impact Assessment (DPIA).

Where data is not being processed under EU General Data Protection Regulation Article 9, there is a limited right for the controller to retain the data after the app is deleted.

Use of patient held devices and apps may require Medicines & Healthcare products Regulatory Agency (Medicines and Healthcare Products Regulatory Agency) approval.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ understand that the provider of the device may be either a controller or a processor
- ✓ consider how a lawful exemption for special category data under General Data Protection Regulation article 9 (see glossary) is going to be met, especially where the intention is to depend on explicit consent as the lawful basis for processing
- ✓ understand whether or not the device or app falls within the Medicines and Healthcare products Regulatory Agency regulations and requires certification.

Should not:

- ✓ underestimate the standard of explicit consent required to achieve compliance remotely through a device or an app.

What needs to be done?

To make use of patient held devices and apps, you need to:

- ✓ complete data flow mapping, noting data controller and processor relationships
- ✓ complete required Data Protection Impact Assessment(s), including an assessment of how individuals will be able to exercise their rights
- ✓ carry out supplier due diligence
- ✓ ensure adequate safeguards are in place, security testing is carried out and data integrity is assured across systems and devices
- ✓ ensure processes are in place to obtain consent and manage withdrawals or changed preferences
- ✓ complete the communications programme.

Medicines & Healthcare products Regulatory Agency: "Medical devices regulation and safety"

Medicines & Healthcare products Regulatory Agency: "Guidance: Medical device stand-alone software including apps (including IVDMDs)" (2017)

Public Health England: "Guidance: Criteria for health app assessment" (October 2017)

European Union Agency for Network and Information Security: "Privacy and data protection in mobile applications" (November 2017)

Internet of Things

Context

The **Internet of Things Test Beds** sought to realise the benefits of environmental monitoring and insight rich datasets created by integrated devices. **Technology Integrated Health Management** brought together a range of devices to provide a holistic view of a patient's current and trending status, to monitor and assess in real time while also informing more tailored care plans. Meanwhile, **Diabetes Digital Coach** sought to improve the Internet of Things method, making better use of collected data by creating a platform to share this data across applications, to reduce the required number of devices.

The Internet of Things, also referred to as the health related Internet of Things (Health-IoT), encompasses devices that monitor and collect data about individual patients to improve health outcomes, support medical staff and enable earlier intervention.

The data collected is used to inform health and social care professionals about a range of different aspects of a person's life, environment and responses. This may involve matching and analysing data from a range of devices operated by different suppliers to build a profile of the individual's physical or mental health and behaviour to help in making a diagnosis, as well as personalised medical and lifestyle treatment options.

What are the information governance implications?

Data security is a particular concern. Data from wearable and implantable devices may be transmitted in real time to health care professionals. **Technology Integrated Health Management** sought to leverage Internet of Things technology during Wave 1 and were required to undertake security testing prior to commencing the project and validation of data destruction as part of project close down.

Specific risks to individuals include the loss of personal confidential health data, clinical risk resulting from corrupted data, and external security threats such as hacking. Risks are often increased because of low technical awareness among users and where data is further shared with third parties for analysis or research.

Useful Links

NHS Digital:
"Data and cyber security: protecting information and data in health and care"

Internet of Things UK:
"Internet of Things in Health and Social Care Preserving Privacy: Good Practice Brief" (November 2017)

PETRAS Internet of Things Research Hub

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ be able to communicate to users the personal implications of the implementation and application of Internet of Things devices in their home
- ✓ map data flows between devices, and the message structure, to understand whether the data is personal data or not
- ✓ understand the risk of device hacking and the security considerations.

What needs to be done?

To use Health-IoT or Internet of Things without increasing risks of loss of confidential data, you must:

- ✓ complete data flow mapping, noting data controller and processor relationships
- ✓ complete required Data Protection Impact Assessment(s) , including an assessment of the impact on the right to a private family life under Article 8 of the Human Rights Act
- ✓ understand and plan for other regulatory activities required for health research (Health Research Authority) and medical device regulation (Medicines and Healthcare products Regulatory Agency)
- ✓ carry out supplier due diligence
- ✓ ensure adequate safeguards are in place, security testing is carried out and data integrity is assured across all systems and devices
- ✓ develop the system following principles of data protection by design and by default

European Union Agency for Network and Information Security:
"A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment" (March 2018)

Article 29 Working Party on Data Protection:
"Opinion 8/2014 on Recent Developments on the Internet of Things", adopted 16 September 2014

Technology enabled delivery models

Context

Care City, Perfect Patient Pathway, Technology Integrated Health Management and Lancashire and Cumbria Innovation Alliance sought to use mobile technology to improve the efficiency of service delivery and support. Combining typical care plans with additional resources such as online communities for patients (Care City) and long distance check-ups such as TeleCare technologies (LCIA) can greatly improve overall care quality and patient independence – minimising demand for more costly services such as A&E.

Technology-enabled delivery models, also known as technology-enabled care services or TECs, is the delivery of healthcare at a distance; for example, through the use of telehealth, telecare, telemedicine and self-care apps. Services include call centres and online resources, such as NHS 111, remote consultations, e-visits or video conferences between health professionals.

What are the information governance implications?

The **Care City** site sought to use technology enabled delivery in combination with several other technologies including online communities for patients with specific conditions. Use of multiple technologies across several providers identified a common set of information governance implications for future sites, requiring evaluation and documentation of:

- how each technology enabled model is using personal data and special categories of data
- the location of processing
- whether any recordings will be made
- any access by third party service providers.

The integrity of the equipment and connection should be tested for resilience against threats, such as hacking, interception or introduction of malware or spyware.

Additional risks include:

- the quality of sound and image transmissions not being of a suitable standard
- unauthorised third parties having access to the personal data being communicated – for example, by access to records or logs or through the presence of third parties off-camera during video consultations.

Useful Links

NHS England:
"Technology Enabled Care Services (TECS)" (2015)

NHS Digital:
"Clinical Risk Management: Telehealth / Mobile Health Solutions – Implementation Guidance" (2013)

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ consider how technologies can enable effective delivery of integrated health and social care delivery, supported by joined up data across services and devices
- ✓ carry out data flow mapping to understand how inter-operability of systems creates information governance risks to both legislated privacy and the common law duty of confidentiality.

Should not:

- ✓ confuse data sharing and processing relationships with commercial arrangements with technology partners.

What needs to be done?

To use technology-enabled health and care delivery services, you need to:

- ✓ complete data flow mapping
- ✓ complete required Data Protection Impact Assessment(s)
- ✓ carry out supplier due diligence
- ✓ draw up data sharing agreements and data processing contracts
- ✓ develop a process for managing consent and opt-outs
- ✓ complete the communications programme.

"Data and cyber security: protecting information and data in health and care"

Information Governance Alliance:
"Using Video Conferencing for Service User Consultations" (2016)

Technology enabled research and evaluation

Context

The **Care City Test Bed** sought to work in partnership with Join Dementia Research (JDR) with a view to signing up data subjects to participate in clinical research through the use of their data. Patient consent is a key area to address from an information governance perspective, however, engaging in research as part of an innovation project, also introduces the need to consider the requirements of the Health Research Authority.

The Health Research Authority distinguishes three categories of investigative projects:

- **Research** is designed and conducted to generate new knowledge and may require NHS Research Ethics Committee (REC) approval
- **Audit** is designed to answer the question 'does this service reach a predetermined standard?'
- **Evaluation** is designed to answer the question 'what standard does this service achieve?'

Due to the pioneering nature of their work, Wave 1 Test Bed sites such as, **Perfect Patient Pathway and Diabetes Digital Coach** encountered new questions over whether and how they needed to communicate and coordinate with Health Research Authority. Each future test bed should determine and then plan for their Health Research Authority coordination work stream as early as possible. There are some helpful resources on the Health Research Authority website included in the link section below, with the link to an automated decision tool on how best to classify a Test Bed in terms of Health Research Authority interest being included.

Useful Links

NHS Health Research Authority:
"Is my study research?"

NHS Health Research Authority:
Decision Tool

NHS Health Research Authority:
"Health Research Authority guidance on the General Data Protection Regulation"

What are the information governance implications?

Different regulatory frameworks and approvals apply to each process, so it is important to identify which category the research project falls into as early as possible.

Work is underway on drafting a code of conduct for health research under EU General Data Protection Regulation Article 40 – see glossary. A consultation draft will be released for comment in autum 2018.

Since 25 May 2018, individuals have been able to set national data opt-outs so that confidential health and care information about them will not be used for the purposes of planning and research.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ utilise the tool on the Health Research Authority website to determine whether the proposed project constitutes research, or not
- ✓ consider whether the unique nature of a Test Bed or initiative actually fits into existing Health Research Authority scenarios
- ✓ consult and seek approvals from Health Research Authority if required
- ✓ consider the possibility of an exemption if devices are developed in-house by health bodies.

What needs to be done?

If you plan to conduct some kind of investigative project, you should:

- ✓ determine whether this is research or evaluation
- ✓ complete data flow mapping
- ✓ complete Data Protection Impact Assessment(s)
- ✓ carry out supplier due diligence
- ✓ draw up data sharing agreements and data processing contracts
- ✓ develop a process for managing opt-outs
- ✓ complete the communications programme.

NHS Health Research Authority:
"Templates. Recommended wording to help you comply with General Data Protection Regulation"

NHS Health Research Authority: "Confidentiality Advisory Group (CAG)"

Devices and apps for professionals

Context

In addition to enabling patients to better self-manage their conditions through making support and information more accessible, professional apps and devices can be used to collect and analyse data to provide a more nuanced set of insights to drive diagnosis and care planning. **Perfect Patient Pathway, Diabetes Digital Coach and Lancashire and Cumbria Innovation Alliance** all sought to create and utilise this added level of intelligence through the deployment of integrated applications to better assess issues such as early signs of memory loss and effective management of blood sugar levels.

Many applications used by professionals are classified as medical devices. Medical devices are subject to Medicines & Healthcare products Regulatory Agency (MHRA) approval.

A 'medical device' is defined in Article 1 of Council Directive 93/42/EEC and in UK law under The Medical Device Regulations 2002 (Statutory Instrument Number 618) as:

'an instrument, apparatus, appliance, material or other article, whether used alone or in combination, together with any software necessary for its proper application, which –

1. Is intended by the manufacturer to be used for human beings for the purpose of
   i. Diagnosis, prevention, monitoring, treatment or alleviation of disease
   ii. Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap
   iii. Investigation, replacement or modification of the anatomy or of a physiological process, or control of conception.
2. Does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means.'

Apps which only have administrative functions, such as managing appointments, are unlikely to be classed as medical apps.

What are the information governance implications?

The following must be considered:

- data security, particularly in relation to mobile devices
- what happens to a device at the end of its life
- whether it is a critical device; if it is, what safeguards are in place when the battery runs out, internet connection is lost or compromised
- how the data is transferred from device to the medical record.

Medical Device Regulations are changing in the UK from May 2020.

Test Beds will need to plan for this change as it introduces changes such as more complexity around device classification, a rigorous quality management process, and new rules for software development.

Useful Links

NHS England:
"Technology Enabled Care Services (TECS)"
(2015)

Lessons learned from Wave 1 of the Test Beds programme

Several wave 1 sites, including the **Perfect Patient Pathway and Diabetes Digital Coach** sought to leverage apps for professionals within their Test Beds. Learning from those sites suggests future projects

Should:

- ✓ give careful consideration to whether or not the device or app comes within the Medical Device Directive or Regulation and requires Medicines and Healthcare products Regulatory Agency approval; new legislation is coming into effect in May 2020 that will mean more apps are classified as medical devices
- ✓ understand that, if the device is giving remote access to existing data without an interpretive layer, it is possibly not a device under Medicines and Healthcare products Regulatory Agency consideration.

Should not:

- ✓ always assume Medicines and Healthcare products Regulatory Agency approval is required – typically this is only required where there is no access to the data and the calculations could not be completed by a person. It is important to check and make a determination as early in a programme as possible.

What needs to be done?

Some apps retain data from the previous time they were used, so it is important to confirm that the information being used refers to the current patient. If you plan to use a medical device, you should also:

- ✓ complete data flow mapping
- ✓ required complete Data Protection Impact Assessment(s)
- ✓ decide what level of Medicines and Healthcare products Regulatory Agency engagement is required for a Test Bed
- ✓ carry out supplier due diligence
- ✓ draw up data sharing agreements and data processing contracts
- ✓ implement privacy by design and by default
- ✓ complete the communications programme
- ✓ record the device on the information asset register
- ✓ instigate a business continuity, contingency and recovery process in the event of any loss, damage or loss of access.

NHS Digital:
"Clinical Risk Management: Telehealth / Mobile Health Solutions – Implementation Guidance" (2013)

Medicines & Healthcare products Regulatory Agency: "Medical devices regulation and safety"

Medicines & Healthcare products Regulatory Agency:
"Guidance: Medical device stand-alone software including apps (including IVDMDs)" (2017)

Public Health England:
"Guidance: Criteria for health app assessment" (October 2017)

Technology enabled social prescribing

Context

The **Care City Test Bed** sought to use social prescribing to utilise the impact of community support, shared experiences and knowledge sharing to improve engagement among patients as well as provide a more efficient avenue for support. The common networks allowed people to work together to take medical advice and apply it through peer review and support to improve overall uptake and engagement with care plans and lifestyle changes through the sharing of more tangible success stories.

Social prescribing enables GPs, nurses and other primary care professionals to refer people to a range of local, non-medical services. It is sometimes referred to as community referral.

Social prescribing, therefore, involves a range of organisations with varying levels of resources and levels of expertise. Experience from the **Lancashire and Cumbria Innovation Alliance and Care City Test Beds** demonstrated that early completion of specific Data Protection Impact Assessments was critical in determining what personal data can be securely shared between partners to the project.

What are the information governance implications?

In most cases of social prescribing, the organisation making the referral (or prescription) will be the data controller. The data processor will be the individual or organisation providing the prescribed service. The process of making the referral will almost always necessitate the flow of personal data from the prescribing authority to the service provider. Both parties therefore have a legal duty to ensure they comply with current legislation.

Many service providers may not be part of the formalised health and care sector and may not have access to sufficient information governance capability and capacity to ensure they are able to meet the legislative requirements. This can present a risk when considering processing activity to support social prescribing models.

Useful Links

The Kings Fund:
"What is social prescribing?

Information Governance Alliance:
"Sharing Information about patients and service users with the voluntary sector" (2015)

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ ensure providers of non-medical services understand and prioritise information governance requirements from the outset
- ✓ establish what level of personal data is being processed.

Should not:

- ✓ overestimate the risks in these technologies – in Wave 1 Test Beds, a number of technologies were found to not be processing personal data.

What needs to be done?

Projects that make use of community referral services should:

- ✓ ensure that clear and accessible communications are in place so that individuals understand how, and with whom, their data will be shared and are aware of any risks to personal privacy
- ✓ evaluate potential providers of non-medical services in the context of their relative information governance knowledge, skills and resource
- ✓ consider implication of evaluation findings on requirements for additional information governance resource within project planning.

Section 03

Information Governance enablers

Successful information governance approaches depend on a number of core enablers. This section describes the key tools that can support a future wave of Test Beds programme/project managers and information governance leads to undertake their work. These tools are:

Data flow mapping

The process of documenting the proposed project structure, the relationships between parties and the implications for the transfer and processing of data; this process is the basis for the completion of a Data Protection Impact Assessment.

Data Protection Impact Assessments

A tool to help identify and minimise data protection risks within a project. Under the General Data Protection Regulation, Data Protection Impact Assessments are mandatory for processing personal information and should be reviewed throughout the lifecycle of a project. The Data Protection Impact Assessment is intended to be a 'living document' and should be regularly reviewed and updated by programmes.

Data processing contracts

Where a controller/processor relationship exists, a data processing contract is required to govern processing activity and document the controls in place to protect data.

Data sharing agreements

These set out a common understanding between data controllers to govern the sharing of data.

Communications and transparency

Recent legislative changes have increased the requirements for effective communication and transparency. A data subject must be informed of how their data is used.

Data flow mapping

Context

Data flow mapping is a prerequisite for effective approaches to information governance; it is closely tied to the accompanying Data Protection Impact Assessment. A good data flow map identifies the data assets (data at rest) and data flows (exchanges of data) that enable the relevant objective or initiative to be delivered.

Data flow mapping is a specialist skill and should be supported by information governance professionals wherever possible. Wave 1 Test Beds were required to carry out detailed flow mapping as the first step in understanding their information governance risks. In some cases, this was locally driven and in others, external expertise was sought to guide the process and ensure all flows were documented and accounted for.

Two processes need to be recorded in data flow maps:

1. The actual exchanges of data – physically or digitally – between technologies and people through which key roles (including the status of data controller and data processor) are defined.
2. The legal basis for each transfer of data between parties.

Once complete, data flow maps will have different characteristics; each can be used to clearly assess and attribute the different levels of risk. In turn, these insights are used to inform a Data Protection Impact Assessment which should document the activities required to mitigate risks and ensure that processing is both lawful and proportionate.

What are the information governance implications?

Data flow maps are an essential foundation for all other information governance activity as it relates to the sharing and/or processing of personal data. They should be maintained and updated throughout the life of the project.

It is important to recognise that data flow mapping, and the identification of legal basis for processing, should be considered in the context of a data subject (individual's) rights and not be driven by organisational strategic and operational concerns.

A key issue to address when mapping data flows is to identify and assign controller and processor relationships for each processing activity. Guidelines on how to do this are being drafted by the IGA for future publication. In the meantime, the resources outlined below should help to provide a suitable foundation.

Please note that the ICO guide was drafted under the 1998 Data Protection Act and includes references to 'Controllers in Common'. The General Data Protection Regulation and 2018 Data Protection Act do not recognise the concept of 'Controllers in Common'. Data maps should only indicate 'Controller', 'Joint Controller' 'Processor' and 'Sub-processor'.

Useful Links

Information Commissioner's Office:
General Data Protection Regulation Guidance – Documentation

Information Governance Alliance:
General Data Protection Regulation: Guidance on lawful processing

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ prioritise the execution of high level data flow maps as part of documenting the proposed project structure
- ✓ engage with information governance resource from the outset to map roles and responsibilities of all partners
- ✓ take a granular approach (in some cases field by field) to the production of data flow maps.

What needs to be done?

When carrying out data flow mapping, you should:

- ✓ complete this at the outset of the project and maintain it throughout the project's lifecycle
- ✓ if required, arrange training on data flow mapping techniques
- ✓ identify any existing data flow mapping templates within your organisation(s)
- ✓ find out whether any data flow mapping has already been undertaken as part of the project set up
- ✓ identify suitably qualified information governance expertise to guide and quality assure the data flow mapping process and associated outputs.

Data Protection Impact Assessments

Context

Under the General Data Protection Regulation, Data Protection Impact Assessments replace Privacy Impact Assessments (PIAs) as the vehicle by which proposed flows of personal identifiable data are governed, and controls developed, to ensure lawful processing.

DPIAs form the basis of project design and must address the privacy by design and privacy by default requirements of the EU General Data Protection Regulation.

There are two stages:

1. An initial evaluation of the degree of risk, informed by data flow mapping, to determine the depth to which a Data Protection Impact Assessmentmust be executed.
2. Where the proposed processing is likely to result in a 'high risk to the rights and freedoms of individuals', a full assessment of privacy risks and mitigating activity.

The vast majority of data processing in a health and social care context will involve special categories of data and it is therefore recommended that a full Data Protection Impact Assessment is carried out. The nature of pre and post General Data Protection Regulation processing under Wave 1 sites meant that commitment to the maintenance and upkeep of Data Protection Impact Assessments varied across sites. Experience shows that as a matter of good governance, wider project management should make provisions for regular reviews of Data Protection Impact Assessments to avoid any "surprises" during the life of a project.

What are the information governance implications?

Alongside data flow mapping, Data Protection Impact Assessments must be carried out at the earliest possible opportunity and can be used to identify information governance capacity and capability requirements.

Data Protection Impact Assessments identify risks; risk mitigating controls should be proportionate to the risk identified. If a risk is identified that cannot be mitigated, the ICO must be consulted before processing commences. They will normally provide advice within eight weeks; 14 weeks in complex cases.

Useful Links

Information Commissioner's Office:
Data protection impact assessments

Health Research Authority:
Data Privacy Impact Assessments

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ complete Data Protection Impact Assessments for each data flow at the earliest opportunity
- ✓ engage all partners in the development of the Data Protection Impact Assessment(s)
- ✓ review the Data Protection Impact Assessment at periodic intervals throughout the lifecycle of the project.

Should not:

- ✓ overlook the critical importance of the Data Protection Impact Assessment as the key document in recording decisions with regard to whether the proposed processing involves personal data.

What needs to be done?

When carrying out Data Protection Impact Assessments, you should:

- ✓ ensure these are completed at the start of each initiative and are informed by your data flow mapping
- ✓ identify/create and agree on a standard template which meets Article 29 (see glossary) requirements
- ✓ publish the completed Data Protection Impact Assessment to your website and your records of processing activity
- ✓ Consider the need for redaction of sensitive topics when sharing or publishing the Data Protection Impact Assessment.

Data processing contracts

Context

All Wave 1 sites involved data processing on behalf of a data controller by a data processor.

- A **data controller** is the person or agency who determines the purposes and means of the data processing activity
- A **data processor** is the person or body that processes the data on behalf of the controller.

Where data flow mapping identifies instances where data is processed by a data processor on behalf of a data controller, a legally binding written data processing contract is required. This should include clauses appropriate to the processing risks identified (highlighted in the Data Protection Impact Assessment), as well as mandatory clauses for all data processing contracts. Experience from Wave 1 Test Beds showed that the time taken to draft and agree Data Processing Contracts took significantly longer than originally planned for. This meant that some sites were restricted in the amount of "live time" they have for testing the proposed innovative interventions.

Typically, a controller will assess the processing activity and risk-assess the processor, imposing clauses proportionate to that risk.

Importantly, the EU General Data Protection Regulation creates new duties for the processor. Contracts drawn up and agreed before the General Data Protection Regulation enforcement date are unlikely to be valid under the new regulation.

What are the information governance implications?

The requirement for legally binding contracts typically invokes a related requirement for advice from qualified information law practitioners.

Where the data flow mapping and Data Protection Impact Assessment process identifies the need for a data processing contract, projects need to provide sufficient resources and allow lead times for drafting and agreeing contracts.

Typically, data processing contracts will need to address detailed descriptions of the type of data to be processed, the nature of processing activity, including the duration, and the obligations and rights of both controller and processor.

Useful Links

Information Commissioner's Office:
Office: Contracts

NHS procurement transparency:
NHS Standard Contract

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ use data flow mapping and the Data Protection Impact Assessment(s) to determine whether a data processing contract is required
- ✓ ensure mandatory clauses under General Data Protection Regulation are incorporated when drafting contracts.

Should not:

- ✓ overlook the critical importance of the Data Protection Impact Assessment as the key document in recording decisions with regard to whether the proposed processing involves personal data.

What needs to be done?

When completing data processing contracts, you should:

- ✓ map the data flows to understand if there are data controller/data processor arrangements
- ✓ agree outline terms between parties before seeking legal counsel
- ✓ draft clauses that address risks identified in the Data Protection Impact Assessment
- ✓ use existing templates where possible
- ✓ check final drafts using checklist tool (signpost)
- ✓ publish to website and in records of processing activity.

Government Public procurement policy.
Directives, regulations, policies and guidance relating to the procurement of supplies, services and works for the public sector

Procurement and contracting transparency requirements. Guidance to assist departments in meeting the procurement and contracting transparency requirements

Data sharing agreements

Context

Data sharing agreements are only valid between data controllers – those who determine the purposes and means by which personal data can be processed. They should not be confused with data processing contracts which govern relationships between controllers and processors (those who undertake the processing of data on behalf of a controller).

Data sharing agreements are strongly recommended although they are not a legal requirement. They set out specific concerns relating to the data to be shared, as identified through data flow mapping and Data Protection Impact Assessment exercises. Due to the nature of Wave 1 Test Bed sites and the relationship between Data Controllers (typically Health service providers) and Data Processors (either Health Service Providers or commercial technology partners), flows of data were, for the most part, governed by Data Processing Contracts, rather than Data Sharing Agreements. That said, future projects may have shared determination over the treatment of data and would therefore wish to consider a Data Sharing Agreement to govern those flows.

Under the EU General Data Protection Regulation, parties will need to satisfy requirements around accountability, transparency and communications and be assured of each other's commitment to meeting those duties. Data sharing agreements can be a tool to help demonstrate accountability and commitments between parties.

What are the information governance implications?

When drafting data sharing agreements, particular attention should be paid to the new duties around communication and transparency under the EU General Data Protection Regulation; articles 12, 13 and 14 (see glossary) of the legislation provide detailed guidance with regard to these requirements.

The new legislation places heightened emphasis on the level of detail advised for data sharing agreements, including field by field breakdowns of the data to be shared. This level of detail should be replicated in communication materials to ensure the subject is fully aware of how their data will be shared.

Useful Links

Information Commissioner's Office:
Accountability and governance

Information Commissioner's Office:
General Data Protection Regulation Guidance – Documentation

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ use data flow mapping and the Data Protection Impact Assessment to determine what is required from a data sharing agreement
- ✓ carefully consider the principles of lawfulness, fairness and transparency when drafting data sharing agreements.

Should not:

- ✓ confuse Data Sharing Agreements (between controllers) with Data Processing Contracts (between controller(s) and processor(s)).

What needs to be done?

When completing data sharing agreements, you should:

- ✓ first complete data flow mapping to verify the controller-to-controller data sharing to be addressed in the agreement
- ✓ complete a Data Protection Impact Assessment to identify the specific risks associated with sharing and the activity required to mitigate them
- ✓ include standard rules and obligations for each party to address the risks identified
- ✓ use existing templates where possible, but verify against current requirements (specifically the General Data Protection Regulation and the Data Protection Act 2018)
- ✓ check final drafts using checklist tool.

National Data Guardian for Health and Care: "Information: To Share Or Not To Share? The Information Governance Review" (2013)

Communications and transparency

Context

The EU General Data Protection Regulation specifies that individuals must be provided with information about the data controller, how their personal data is used and managed, and how to exercise their rights; this is referred to as 'fair processing'.

In common with many organisations, partners within Test Bed sites typically overlooked the increased importance of accessibility and transparency around data processing activity under the General Data Protection Regulation. This is a significant undertaking, particularly where projects propose to rely on explicit consent as the basis for processing.

The information must be provided in clear language, be accessible to the intended audience and provided at the time when the data was obtained, or – if the information is obtained from a third party – at a 'reasonable time after obtaining the personal data, but no later than one month'.

What are the information governance implications?

Fair processing notices must explain the nature of processing in plain language that patients can understand. The controller and processor must satisfy themselves that the data subject understands how their data is being used. To ensure the information is accessible to all potential audiences, it may be necessary to use multiple formats and communication channels. This could include easy read versions, translations and notices suitable for children.

Useful Links

Information Commissioner's Office:
"The Right to be Informed"

NHS Identity guidelines

NHS Accessible Information Standard
Making health and social care information accessible

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ embed information governance related communications and transparency requirements within the overarching project communications strategy at the earliest opportunity
- ✓ carry out research with potential data subjects to understand how they would access fair processing information in practice.

What needs to be done?

- ✓ complete data flow mapping
- ✓ complete Data Protection Impact Assessment including identifying communication methods suitable for the intended audience
- ✓ develop and implement a communications and transparency strategy.

Wellcome Trust:
"The one-way mirror: public attitudes to commercial access to health data" (2016)

Wellcome Trust:
Understanding patient data

Health Research Authority:
Informing participants and seeking consent

Section 04

4. Key issues for consideration

This section addresses the core lessons learned during Wave 1 of the Test Beds programme.
Each area explores the context, specific lessons and any considerations or actions you should be aware of in your role.

Each of the areas detailed below were observed in at least two Wave 1 Test Bed sites and some were prevalent across all sites, to a greater or lesser degree. The content in this section has been carefully designed to aid future technology led innovation projects and more specifically, has been tailored to support the two key roles of project/programme manager and information governance lead. Useful resources, based on the experience of Wave 1 sites, are signposted throughout.

Local information governance Capability and Capacity

Identifying and engaging local information governance support has proven to be critical to project success.

Evaluating Technology Partners

Evaluating and selecting technology partners on the basis of their information governance capability through due diligence exercises.

Privacy by Design

Privacy by Design describes the embedding of an approach and mind-set, during the planning and design stages of a project, that seeks to identify and implement the correct tools and processes to maximise privacy into the foundation of a technology solution.

Privacy by Default

Privacy by Default is the proactive implementation of the strictest privacy settings by default into the tools and processes created through the privacy by design approach to maximise compliance.

Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) are powerful examples of the tools available to incorporate into solutions via the privacy by design approach – both minimising and mitigating risks associated with privacy compliance.

Legal Counsel

In some cases, the complexity of projects may determine a requirement to seek legal counsel.

Programme or project manager: key issues

The content of this section has been developed for two different audiences, programme or project managers and information governance staff.

This sub-section provides tailored information governance support for programme or project managers.

You are a non-specialist programme or project manager.

You would like an overview of the lessons learned from the first wave of Test Bed sites. You need to understand information governance requirements in sufficient detail to be able to plan effectively and to ensure that information governance enables and supports your project.

Local information governance knowledge, skills and resources

Context

Identifying and engaging local information governance support early is critical to the success of a project; you will need to sponsor and champion this engagement. New projects must anticipate, identify and address key information governance issues at the outset and throughout its life. They should ensure that all project stakeholders recognise the significance of information governance for the success of the project.

As soon as the proposed project structures and the relationship between parties have been defined, information governance practitioners should carry out an initial risk assessment. As a minimum, this should include high level data flow mapping to identify risks in the use of data from which people can be identified.

The overall project management portfolio needs to include a information governance project plan and an estimate of the resources required to carry it out.

Useful Links

Information Governance Alliance:
General Data Protection Regulation guidance

Information Governance Alliance:
Information governance is the responsibility of everyone

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ engage at the earliest opportunity with information governance expertise
- ✓ ensure information governance is recognised by all project stakeholders as a key enabler of project success
- ✓ work with information governance staff to scope likely requirements for information governance input across the project lifecycle
- ✓ sponsor direct information governance participation and reporting to project governance group(s).

Should not:

- ✓ proceed beyond project initiation without having identified and consulted with information governance staff
- ✓ only involve information governance staff at the outset of the project.

What do I need to do?

When planning to access information governance expertise to support projects, you should:

- ✓ identify and engage an information governance staff at the earliest opportunity
- ✓ carry out initial data flow mapping exercises as soon as the proposed relationships between parties and data needs can be identified
- ✓ use the results of this exercise to carry out an initial evaluation of the risks presented by the proposed data usage
- ✓ work alongside identified information governance expertise and establish a information governance project plan with an estimate of the resources required.

Information Governance Alliance:
Changes to Data Protection legislation:
why this matters to you (CEO briefing)

Information Governance Alliance:
New to care sector information governance?
What you should know

Information Governance Alliance:
General Data Protection Regulation guidance –
frequently asked questions

Evaluating technology partners

Context

Evaluating and selecting technology partners is a complex process. Where projects will involve multiple partners with a variety of technology solutions, a set of information governance criteria – informed by the documents listed below – can help the selection process.

Projects should ensure partners have sufficient expertise and resources to comply with appropriate organisational and technical standards. Building this into the initial evaluation can avoid complex redesigns or repeated procurement exercises and help to meet project timelines and objectives.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ include information governance capability as a key area for assessment
- ✓ emphasise the importance of continual engagement with information governance throughout the project
- ✓ specifically require information governance review and sign-off of any scope or design amendments
- ✓ ensure that information governance oversight is not designated as the sole responsibility of the host organisation.

Useful Links

Information Commissioner's Office:
Data Protection Fee

NHS Digital:
Data Security and Protection Toolkit

Information Commissioner's Office:
General Data Protection Regulation Guidance – Documentation

What do I need to do?

When undertaking the partner selection process, the minimum requirements for reviewing and evaluating their information governance compliance include:

- ✓ Ensuring they are registered with the Information Commissioners Office if so required, such as holding the role of a data processor or controller
- ✓ Ensuring that security and penetration testing certificates are in place for technology partners especially for solutions using patient data
- ✓ NHS Data Security Protection Toolkit (DSPT) completion and/or evidence of compliance with a similar standard, such as ISO27001 – an international standard for Information Security Management Systems
- ✓ evidence of good corporate governance, including documented schedules for reviewing and updating policies and procedures.
- ✓ resources and expertise, including a copy of the job description for the Data Protection Officer (DPO) (or similar role if the DPO is not a statutory role for the supplier)
- ✓ details of any data breaches, including procedures to detect and report data breaches and near misses
- ✓ detailed records of existing and proposed processing activity, such as processing activity outside the European Economic Area
- ✓ evidence of compliance with relevant regulatory standards
- ✓ security testing to recognised standards by a competent organisation.

Information Governance Alliance:
Guidance on the role of the Data Protection Officer

Information Governance Alliance:
Guidance on accountability and organisational priorities

Information Governance Alliance:
Personal data breaches and notification [not yet published]

Privacy by design

Context

Privacy by Design describes the embedding of an approach and mind-set, during the planning and design stages of a project, that seeks to identify and implement the correct tools and processes to maximise privacy into the design of a technology solution. This is instead of seeking to protect privacy as a final layer of security at the end of implementation.

From a practical perspective, the key documents underpinning a privacy by design approach are the data flow maps and Data Protection Impact Assessments, described in this document's glossary and Information Commissioners Office link below. These identify the key areas of risk as well as the degrees of protection required to ensure compliance. This in turn helps guide the solution design, aiding in the identification and implementation of tools and processes that minimise risk and maximise the privacy of data subjects.

The General Data Protection Regulation requires consideration of these factors in the Data Protection Impact Assessment process because:

- potential problems are identified at an early stage, when addressing them will often be simpler and less costly
- processing personal data should be minimised
- organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act
- processing is less likely intrude on the privacy of individuals or have a negative impact on them.

Useful Links

Information Commissioner's Office:
Data protection impact assessments

Health Research Authority:
Data Privacy Impact Assessments

Information Commissioner's Office:
General Data Protection Regulation Guidance –
Data protection by design and default

European Union Agency for Network and
Information Security:
Privacy by Design

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ complete a Data Protection Impact Assessment at the earliest opportunity
- ✓ review the Data Protection Impact Assessment periodically throughout the lifecycle of the project to ensure that controls continue to reflect evolving risks
- ✓ review data flow maps with information governance Information Governance teams to identify opportunities to embed privacy enhancing technologies.

Should not:

- ✓ consider the Data Protection Impact Assessment to be a "one-off exercise" at the outset of the project.

What do I need to do?

When considering a privacy by design approach for your project, you should:

- ✓ refer to the available guidance on privacy by design, such as those in the accompanying links
- ✓ complete a Data Protection Impact Assessment as soon as possible within the project lifecycle to ensure the rights and freedoms of the data subject are protected
- ✓ review the Data Protection Impact Assessment regularly in the light of changes to the project structure or current legislation and guidance around best practice.

Article 29 Working Party on Data Protection: "Opinion 8/2014 on Recent Developments on the Internet of Things"

Information Governance Alliance:
Privacy by design and default [not yet published]

NHS Digital:
Data and cyber security: protecting information and data in health and care

Privacy by default

Context

Privacy by Default is the proactive implementation of the strictest privacy settings by default into the tools and processes created through the privacy by design approach to maximise compliance.

This application of the tools and processes describes the way in which the controls are specifically setup by default to maintain privacy and the proportional use of data whenever it is shared, processed or accessed. It is the practical application of a privacy by design approach, seeking to avoid risks involving data that add limited value. Examples include:

- organisational governance and approvals processes
- tools that control role-based access to data platforms
- non-identifiable interactions and transactions as the default.

Once implemented, a process that embeds privacy by default helps to reduce data breaches, as well as providing the path of least resistance through the design and implementation of information governance compliance.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ use the findings of their Data Protection Impact Assessment to identify the necessary organisational and technical controls
- ✓ identify Privacy Enhancing Technologies (PETs) to assist the implementation of privacy controls.

Should not:

- ✓ access or process data fields unnecessary to the identified use of data at the time of collection.

Useful Links

Information Commissioner's Office:
Data protection impact assessments

Health Research Authority:
Data Privacy Impact Assessments

Information Commissioner's Office:
General Data Protection Regulation Guidance –
Data protection by design and default

Article 29 Working Party on Data Protection:
"Opinion 8/2014 on Recent Developments on the Internet of Things", adopted 16 September 2014

What do I need to do?

When considering your approach to privacy by default, you should:

- ✓ identify the greatest threats to the rights and freedoms of data subjects by analysing the risks raised during data flow mapping and Data Protection Impact Assessment
- ✓ work with your information governance staff to identify privacy by default approaches to mitigate those risks, such as role-based access to personal data
- ✓ review your privacy by default approach as a specific element of your periodic Data Protection Impact Assessment reviews to ensure the approach is fit for purpose and reflects changes or revisions to project structures or current legislation.

Information Governance Alliance:
Privacy by design and default [not yet published]

Privacy enhancing technologies

Context

Privacy Enhancing Technologies (PETs) are powerful tools for minimising and mitigating risk. They can offer systems and methods that help to achieve compliance with current data protection legislation and minimise the risk of data breaches relating to personal identifiable data.

Examples of PETs include:

- role-based and identity access management software
- multi-factor authentication to control access to databases and interfaces
- pseudonymisation and anonymization engines
- secure encryption technologies.

Multi-partner projects will need to consider the impact of these technologies when planning mitigating actions to address identified risks. You can find out more about different types of Privacy Enhancing Technologies later in this document; your internal information governance team can help you assess which of these may be most appropriate for your project.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ consider the ways that PETs can support a Privacy by Design and Privacy by Default approach at the outset of the project
- ✓ consult with information governance expertise to identify specific risks where PETs could be used effectively to mitigate threats to privacy
- ✓ conduct market research or engagement exercises, where appropriate, to assess the ability of PETs solutions to mitigate risks.

Should not:

- ✓ overlook the role of PETs in mitigating key project risks.

What do I need to do?

When considering PETs to minimise the information governance risk within your project, you should:

- ✓ work with your information governance leads to specify your project's requirements based on the outcomes of data flow mapping and Data Protection Impact Assessment
- ✓ explore the extent to which partner organisations may already have PET capabilities that could be reused or configured for your project
- ✓ review the external vendor market with your information governance lead to identify and evaluate the solutions on offer.

Useful Links

Information Commissioner's Office:
General Data Protection Regulation Guidance –
Data protection by design and default

European Union Agency for Network and
Information Security:
Privacy enhancing technologies

Article 29 Working Party on Data Protection:
"Opinion 8/2014 on Recent Developments on the
Internet of Things",
adopted 16 September 2014

Information Governance Alliance:
Privacy by design and default
[not yet published]

Legal counsel

Context

When pioneering new and innovative approaches and technologies across a number of medical domains, the flow of data can often be complex. In some cases, the legality of sharing or processing data may be difficult to assess – particularly where there is no precedent for doing so. Advice from legal counsel to support your information governance team's assessment can therefore provide an added assurance regarding the legality of your proposed solution. During Wave 1, the RAIDPlus Test Bed sought legal opinion regarding the proposed flow of pseudonymised patient data from an NHS Trust to a commercial technology partner. The guidance presented below draws heavily on the experience of RAIDPlus partners in navigating this process.

To make efficient use of time and optimise the return on investment in commissioning legal support, you should draw up a clear and concise brief for legal counsel based on the Data Protection Impact Assessment.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ engage all parties in identifying the key information governance risks and proposed mitigating controls

Lessons learned from Wave 1 of the Test Beds programme continued

- ✓ where possible, ensure all parties agree on the objectives for seeking legal counsel
- ✓ ensure the brief is accompanied by your data flow maps and documented Data Protection Impact Assessments, and clearly identify the specific flows and risks on which you are seeking guidance.

Should not:

- ✓ engage legal counsel without having first consulted with local information governance expertise to identify and evaluate terms.

What do I need to do?

If seeking legal counsel for your project, you should:

- ✓ ensure that all parties are clear about the questions, are involved in drawing up the brief and agree on the final version
- ✓ ensure that your information governance experts have been engaged in drafting the brief
- ✓ pending delivery of a legal opinion, plan ahead to understand what impact this might have on the information governance staff needed for the project.

Useful Links

Information Commissioner's Office:
Data protection impact assessments

Health Research Authority:
Data Privacy Impact Assessments

Information governance lead: key issues

The content of this section has been developed for two different audiences, programme or project managers and specialist information governance staff.

This sub-section provides tailored information governance support for information governance specialists

You have experience of working in an information governance capacity.

Your role is to provide advice, guidance and support on strategic and tactical information governance concerns to deliver a project that is compliant with national policy and legal obligations.

Local information governance knowledge, skills and resources

Context

Identifying and engaging local information governance support is critical to the success of a project. Innovative projects need sufficient information governance capability and capacity to anticipate, identify and address key issues at the outset and throughout the lifecycle of a project.

As soon as the proposed project structures and the relationship between parties have been outlined, information governance practitioners should begin making an estimate of the resources that will be required.

At a minimum, this should include:

- completing high level data flow mapping to identify risks
- identifying mandatory legal, regulatory and policy requirements
- ensuring engagement with internal programme stakeholders
- assigning responsibility and embedding processes for information governance reporting and accountability within the project
- conducting an assessment of the likely timescales for completion of legal and policy requirements.

Useful Links

Information Governance Alliance:
General Data Protection Regulation guidance

Information Governance Alliance:
Information governance is the responsibility of everyone

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ prioritise collaboration between information governance expertise and the Project Manager to scope likely requirements for information governance support across the project
- ✓ ensure there is a suitable pool of information governance skills and knowledge to support innovative use of technology.

What do I need to do?

To deliver the necessary information governance staffing to support projects, you need to:

- ✓ identify and define legal, regulatory and policy requirements
- ✓ start the Data Protection Impact Assessment process to identify risks
- ✓ conduct high level data flow mapping (with all stakeholders) to carry out an initial evaluation of the risks presented by the proposed data use
- ✓ work with project management to establish a information governance project plan and estimate resource implications
- ✓ assign responsibility and embed processes for information governance reporting and accountability within the project.

Information Governance Alliance: Changes to Data Protection legislation: why this matters to you (CEO briefing)

Information Governance Alliance: General Data Protection Regulation guidance – frequently asked questions

Information Governance Alliance: Guidance on the role of the Data Protection Officer

Information Governance Alliance: Guidance on accountability and organisational priorities

Evaluating technology partners

Context

Evaluating and selecting technology partners is a complex process. Where projects involve multiple partners with varying technology solutions, a set of information governance criteria – informed by the documents linked below – facilitates the selection process.

Projects should ensure partners have sufficient expertise, resources and product capability to comply with organisational and legislative technical requirements. Engaging with project teams at an early stage to build these requirements into initial partner evaluations can prevent complex redesigns or repeated procurement exercises and help to meet project timelines and objectives.

Delays, scope shifts and compliance risks can also be prevented by working with partners to ensure data processing contracts include mandatory clauses required by the EU General Data Protection Regulation and UK Data Protection Act 2018.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ ensure information governance capability is a key area for assessment and that information governance leads input to this process
- ✓ emphasise the importance of continual engagement with the technology partners' information governance team throughout the project
- ✓ ensure project managers work with information governance leads to embed information governance review and sign-off for any scope or design amendments.

Useful Links

- Information Commissioner's Office: Data Protection Fee
- NHS Digital: Data Security and Protection Toolkit
- Information Commissioner's Office: General Data Protection Regulation Guidance – Documentation
- Information Governance Alliance: Guidance on the role of the Data Protection Officer

What do I need to do?

Information governance practitioners can support projects by advising on criteria to include as part of the selection and tendering process. As a minimum this includes:

- ✓ Information Commissioners Office registration (where applicable)
- ✓ ensure that security and penetration testing certificates are in place for technology partners especially for solutions using patient data
- ✓ Data Security Protection Toolkit completion and/or evidence of compliance with a similar standard, such as ISO27001 – an international standard for Information Security Management Systems.
- ✓ evidence of good corporate governance, including documented schedules for reviewing Data Protection Impact Assessments and updating of policies and procedures
- ✓ resources and expertise, including a copy of the job description for the Data Protection Officer (or similar role if the DPO is not a statutory role for the supplier)
- ✓ details of any past data breaches, including procedures to detect and report data breaches and near misses
- ✓ detailed records of existing and proposed processing activity, such as processing activity outside the European Economic Area, addressing key criteria.

Information Governance Alliance:
Guidance on accountability and organisational priorities

Information Governance Alliance:
Personal data breaches and notification [not yet published]

NHS Digital:
NHS and social care data: off-shoring and the use of public cloud services

Information Commissioner's Office:
Contracts

Privacy by design

Context

Privacy by Design describes the embedding of an approach and mind-set, during the planning and design stages of a project, that seeks to identify and implement the correct tools and processes to maximise privacy into the design of a technology solution. This is instead of seeking to protect privacy as a final layer of security at the end of implementation.

From a practical perspective, the key documents underpinning a privacy by design approach are the data flow maps and Data Protection Impact Assessments, described in this document's glossary and ICO link below. These identify the key areas of risk as well as the degrees of protection required to ensure compliance. This in turn helps guide the solution design, aiding in the identification and implementation of tools and processes that minimise risk and maximise the privacy of data subjects.

The Information Commissioner's Office recognises these benefits of an approach based on privacy by design:

- potential problems are identified at an early stage, when addressing them will often be simpler and less costly
- increased awareness of privacy and data protection across the organisation
- organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act
- actions are less likely intrude on the privacy of individuals or have a negative impact on them.

Useful Links

Information Commissioner's Office:
Data protection impact assessments

Health Research Authority:
Data Privacy Impact Assessments

Information Commissioner's Office:
General Data Protection Regulation Guidance –
Data protection by design and default

European Union Agency for Network and
Information Security:
Privacy by Design

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ identify and agree a common template for Data Protection Impact Assessment completion
- ✓ involve the information governance leads of participating entities in the completion of a Data Protection Impact Assessment
- ✓ review data flow maps to identify opportunities to embed privacy enhancing technologies.

What do I need to do?

Information governance practitioners can support project teams to adopt a privacy by design approach by:

- ✓ ensuring project colleagues are aware of privacy by design guidance produced by the Information Commissioner and EU Article 29 Working Party (A29WP)
- ✓ complete a Data Protection Impact Assessment as early as possible in the lifecycle of the project to ensure the rights and freedoms of individuals are protected
- ✓ regularly review the Data Protection Impact Assessment in light of changes to the project structure, legislation and guidance on best practice to ensure ongoing compliance.

Article 29 Working Party on Data Protection: "Opinion 8/2014 on Recent Developments on the Internet of Things", adopted 16 September 2014

Information Governance Alliance: Privacy by design and default [not yet published]

NHS Digital: Data and cyber security: protecting information and data in health and care

Privacy by default

Context

Privacy by Default is the proactive implementation of the strictest privacy settings by default into the tools and processes created through the privacy by design approach to maximise compliance.

This application of the tools and processes describes the way in which the controls are specifically setup by default to maintain privacy and the proportional use of data whenever it is shared, processed or accessed. It is the practical application of a privacy by design approach, seeking to avoid risks involving data that add limited value. Examples include:

- organisational governance and approvals processes
- tools that control role-based access to data platforms
- non-identifiable interactions and transactions as the default.
- Information Governance practitioners can support project teams to use Data Protection Impact Assessments and Data Flow Maps to identify opportunities to apply Privacy by Default controls.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ emphasise the importance of the Data Minimisation principle from the outset of project design
- ✓ use the findings of the Data Protection Impact Assessment to identify organisational and technical controls needed
- ✓ use data flow mapping and Data Protection Impact Assessments to identify opportunities to incorporate Privacy Enhancing Technologies (PETS) and organisational controls at the design stage.

Useful Links

Information Commissioner's Office:
Data protection impact assessments

Health Research Authority:
Data Privacy Impact Assessments

Information Commissioner's Office:
General Data Protection Regulation Guidance –
Data protection by design and default

Article 29 Working Party on Data Protection:
"Opinion 8/2014 on Recent Developments
on the Internet of Things",
adopted 16 September 2014

What do I need to do?

Information governance practitioners can support project teams in using Data Protection Impact Assessments and data flow maps to identify opportunities to apply privacy by default controls and to put them in to practice by:

- ✓ ensuring project colleagues are aware of privacy by design guidance produced by the Information Commissioner and EU Article 29 Working Party (A29WP)
- ✓ completing a Data Protection Impact Assessment as early as possible in the lifecycle of the project to ensure the rights and freedoms of individuals are protected
- ✓ regularly reviewing this against any changes to the project structure, legislation and guidance on best practice.

Information Governance Alliance: Privacy by design and default [not yet published]

Information Governance Alliance: Guidance on accountability and organisational priorities

Privacy enhancing technologies

Context

Privacy Enhancing Technologies (PETs) are powerful tools for minimising and mitigating risk. They offer systems and methods that help to achieve compliance with current data protection legislation and use technology to:

- minimise the risk of data breaches relating to personal identifiable data
- help to achieve compliance with data protection legislation
- observe and facilitate the privacy rights of individuals.

When conducting the Data Protection Impact Assessment, information governance practitioners can work with project partners to identify the ways in which PETs can offer more efficient ways to address and mitigate risks.

Examples of PETs include:

- role-based and identity access management software
- multi-factor authentication to control access to databases and interfaces
- pseudonymisation and anonymization engines
- secure encryption technologies.

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ consider risks to the rights and freedoms of individuals introduced by novel technologies and data uses and consider balancing these with investment in PETs
- ✓ consider the need for PETs to mitigate risks in discussion with your Caldicott Guardian, Senior Information Risk Owner and Data Protection Officer.

Should not:

- ✓ consider PETs as a solution to fundamental issues in the design and lawfulness of a technical solution or governance framework.

Useful Links

Information Commissioner's Office:
General Data Protection Regulation Guidance –
Data protection by design and default

European Union Agency for Network and
Information Security:
Privacy enhancing technologies

Article 29 Working Party on Data Protection:
"Opinion 8/2014 on Recent Developments on the
Internet of Things",
adopted 16 September 2014

Information Governance Alliance:
Privacy by design and default
[not yet published]

What do I need to do?

Information governance practitioners can support projects by:

- ✓ working closely with Information Technology (IT) leads and procurement teams to establish a clear specification of requirements based on the outcomes of data flow mapping and Data Protection Impact Assessments
- ✓ exploring the extent to which partner organisations may already have PET capabilities that could be reused or configured for your project
- ✓ assisting project management to identify and assess solutions offered by vendors.

Health Research Authority: technical guidance
General Data Protection Regulation: Technical guidance for data protection officers, information governance officers and research governance managers

Legal Counsel

Context

Innovative projects, deploying new technologies across multiple domains, can generate complex data flows.

In some cases, therefore, the legality of processing may be difficult to appraise. In these circumstances, advice should be sought to provide independent assurance regarding the legality of the proposed processing activity. During Wave 1, the RAIDPlus Test Bed sought legal opinion regarding the proposed flow of pseudonymised patient data from an NHS Trust to a commercial technology partner. The guidance presented below draws heavily on the experience of RAIDPlus partners in navigating this process.

If a project decides that it needs legal advice, it is important to prepare thoroughly to that:

- the advice is necessary and timely
- the issues are clearly explained
- any relevant background information is made available
- instructions are drafted that clearly identify specific risk areas where advice is needed
- any advice received is properly incorporated into information governance workstream of the project.

Useful Links

Information Commissioner's Office:
Data protection impact assessments

Health Research Authority:
Data protection and information governance – Currently applicable legislation

Information Governance Alliance:
Guidance on lawful basis for processing

Lessons learned from Wave 1 of the Test Beds programme

Learning from Wave 1 of the Test Beds programme suggests future projects

Should:

- ✓ consult legal counsel only when the parties have reached agreement in principle
- ✓ seek qualified legal advice which can be relied upon to provide additional confidence for stakeholders
- ✓ carefully consider the benefits of using legal counsel to resolve internal disputes pre-contract.

Should not:

- ✓ bring in legal counsel too early
- ✓ consult legal counsel before being able to brief them on the approach agreed by all parties.

What do I need to do?

Information governance practitioners can support projects seeking legal counsel by:

- ✓ using the Data Protection Impact Assessment at an early stage in the project to flag any areas where legal advice or specialist support may be needed
- ✓ identifying any areas of potential conflict between data protection legislation and other laws
- ✓ ensuring the brief for the counsel clearly identifies the specific flows and risks where you need advice
- ✓ challenging yourself on the clarity of the questions posed
- ✓ providing counsel with your data flow maps and Data Protection Impact Assessment
- ✓ working with other stakeholders to identify common issues and prevent duplication of requests for advice
- ✓ pending delivery of a legal opinion, planning ahead to understand what impact this might have on the information governance resources needed for the project.

Information Commissioner's Office: Lawful basis for processing

Health Research Authority: General Data Protection Regulation: technical guidance. Technical guidance for data protection officers, information governance officers and research governance managers

Glossary of terms

Term	Definition
Anonymisation	An irreversible process of turning data into a form which does not identify individuals and where the risk of re-identification is extremely low. When done properly, anonymised data is no longer personal data, and is outside the scope of the General Data Protection Regulation and, common law duty of confidentiality
Automated Decision	Decisions made solely by automated means without human involvement. The rights of an individual in relation to an automated decision only arise where the automated decision can have a legal or significant impact on the individual
Caldicott Guardian	A Caldicott Guardian is a senior person in a health or social care organisation who makes sure that the personal information about patients and service users is used legally, ethically and appropriately, and that confidentiality is maintained. Each NHS organisation is required to have a Caldicott Guardian with specific responsibilities to oversee an ongoing process of audit, improvement and control
Case finding	A process that identifies individuals from a larger population for a specific purpose for example, flu vaccination.
Closed System Processing	This is an isolated system that has no interaction with its external environment. It is also known as 'Black Box Processing'. As there is no direct human interaction with confidential data in a closed system, it can be used as a means of ensuring data are processed without a breach of confidentiality
Common Law Duty of Confidentiality	Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. In practice, this means that all patient/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient/client. Three circumstances making disclosure of confidential information lawful are: • where the individual to whom the information relates has consented • where disclosure is necessary to safeguard the individual, or others, or is in the public interest • where there is a legal duty to do so, for example a court order
Confidentiality Advisory Group (CAG)	CAG is an independent statutory body which provides expert advice to the Health Research Authority and Secretary of State for Health on the use of confidential patient information under the Health Service (Control of Patient Information) Regulations
Controller (previously 'Data Controller')	The natural or legal person, public authority or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data

Term	Definition
Data flow mapping	The identification and recording of information assets and the exchanges of data between assets, internally and with external parties, including the methods of exchange
Data Processor Contract	A written contract between a Controller and Processor setting out the requirements and responsibilities for compliance with data protection legislation. The General Data Protection Regulation sets out specific terms that must be included in the contract as a minimum. Unlike Data Sharing Agreements, contracts are legally binding and may be enforced in a court of law
Data Protection Impact Assessment	DPIAs are a tool to identify and minimise the data protection risks of new projects. They are part of the accountability obligations under the General Data Protection Regulation, and an integral part of 'data protection by default and by design'. Data Protection Impact Assessments that identify high residual risks must be referred to the ICO for approval
Data Protection Officer (DPO)	Unless exempt, the General Data Protection Regulation requires organisations to appoint a data protection officer (DPO). The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. Article 39 of the General Data Protection Regulation (see glossary) sets out the specific tasks of the DPO
Data Security and Protection Toolkit (DSPT)	An online information governance self-assessment tool that enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards. The DSPT must be completed annually by all organisations that have access to NHS patient data and systems to provide assurance that they are practising good data security and that personal information is being handled correctly. The DSPT replaced the information governance Toolkit in April 2018
Data Sharing	The disclosure of data from one or more organisations to a third-party organisation or organisations or sharing data between different parts of an organisation. This can be systematic, routine data sharing for an established purpose, or exceptional, one-off decisions to share data for any of a range of purposes
Data Sharing Agreement (Data Sharing Protocol)	A set of rules adopted by Controller organisations involved in a data sharing operation. There is no statutory requirement for Data Sharing Agreements, but they are regarded as good practice (ICO "Data Sharing Code of Practice")
Data Subject	This is the living individual who is the subject of the personal information (data)
DPA 2018	Data Protection Act 2018. The UK national legislation which supplements the General Data Protection Regulation
Fair Processing	Fair Processing means that personal data must not be processed in a way that is unduly detrimental, unexpected or misleading. To achieve this, people must be aware of how their information will be used. This is done by means of a Privacy Notice
General Data Protection Regulation	The General Data Protection Regulation sets out how organisations must handle personal data. It is part of the wider package of reform to the data protection law that includes the UK Data Protection Act 2018 and EU Law Enforcement Directive 2016/680
GDPR Article 6	Lawfulness of processing
GDPR Article 9	Processing of special categories of personal data

Term	Definition
GDPR Article 10	Processing of personal data relating to criminal convictions and offences
GDPR Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject
GDPR Article 13	Information to be provided where personal data are collected from the data subject
GDPR Article 14	Information to be provided where personal data have not been obtained from the data subject
GDPR Article 17	Right to erasure ("Right to be forgotten")
GDPR Article 20	Right to data portability
GDPR Article 22	Automated individual decision-making, including profiling
GDPR Article 29	Processing under the authority of the controller or processor
GDPR Article 30	Records of processing activity
GDPR Article 39	Tasks of the Data Protection Officer
GDPR Article 40	Codes of Conduct
ICO Registration	The Data Protection (Charges and Information) Regulations 2018 requires every organisation processing personal information as a Controller to pay a data protection fee to the ICO unless they are exempt. Registration information is published on the ICO's Register of Fee Payers
Information Asset	An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles
Information Commissioner's Office (ICO)	The Information Commissioner's Office is the UK's independent supervisory authority under the General Data Protection Regulation. The ICO publishes guidance and investigates breaches of information rights laws
Information Governance	The set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements
Internet of Things	The Internet of Things, also referred to as the Health-related Internet of Things (Health-IoT) is used to refer to devices which monitor and collect data about individual patients to improve health outcomes, support medical staff and enable earlier intervention
Lawful basis	The lawful bases for processing are set out in Articles 6 of the General Data Protection Regulation. At least one of these must apply whenever an organisation processes personal data. If Special Category data are to be processed, at least one condition from Article 6 and Article 9 must apply. The justification for processing must be documented

Term	Definition
Medical Devices	A Medical Device is any instrument, device or software intended by its manufacturer to be used specifically for diagnostic or therapeutic purposes. The Medicines and Healthcare Products Regulatory Agency is the designated competent authority that administers and enforces the law on medical devices in the UK and determines whether a product falls within the definition of a 'medicinal product' or a 'medical device'. Medical Devices are regulated by the Medical Devices Regulations 2002 (SI 2002 No 618, as amended) which enacts the EU Directive 94/42/EEC, and the General Product Safety Regulations 2005 (SI 2005 No 1803)
Opt-out	The qualified option for an individual to choose not to allow their data to be used for the purposes described. The national patient opt-out programme in England ('National Data Opt-out') provides individuals with the opportunity to opt-out of specific non-care related uses of their confidential information. The National Data Opt-out only applies to the disclosure of confidential patient information under the common law duty of confidence, and not to processing under data protection law
Personal Data	Personal data' means any information relating to an identified or identifiable living individual ('data subject')
Population segmentation	Population segmentation is dividing people onto groups according to different characteristics, for example to identify the kind of care they need as well as how often they might need it
Privacy by Default	The implementation of technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose are processed
Privacy by Design	The integration of data protection into processing activities and business practices from the design stage right throughout the lifecycle
Privacy Enhancing Technologies (PETs)	Privacy Enhancing Technologies are technical measures to protect or enhance an individual's privacy, including making it easier for people to exercise their rights
Privacy Notice	Privacy Notices are also referred to a 'fair processing notices'. A Privacy Notice tells people how an organisation collects and uses their information, and how to exercise their rights. The ICO has published a code of practice on Privacy Notices
Processing	Obtaining, recording or holding the data or carrying out any operation or set of operations on data
Processor (previously 'Data Processor')	A person, public authority, agency or other body which processes personal data on behalf of a Controller
Pseudonymisation	Masking or changing personal data so that it can no longer be attributed to a specific data subject without the use of additional information, 'the key'. The key must be kept separately and protected by technical and organisational measures
Public Authority	Any organisation or holder of an office listed in the Freedom of Information Act or designated by order. This includes publicly owned companies as set out in the DPA 2018 section 7
Records of Processing activities	Article 30 of the General Data Protection Regulation (see glossary) requires controllers to keep records of all processing activities involving personal data. The General Data Protection Regulation sets out the minimum information which need to be recorded
Risk Stratification	A systematic process that can be used for commissioning as it divides a population into different strata of risk for a specified outcome, e.g. unscheduled admission to hospital

Term	Definition
Risk Stratification for Case Finding	A systematic process to identify sectors of the population that may benefit from additional clinical intervention, as directed by a lead clinician such as the patient's GP
Role-Based Access Control (RBAC)	Role-Based Access Control restricts access based on a person's role within an organisation and legitimate relationship to the data subject
Section 251	This is a short-hand term and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002. It enables the common law duty of confidentiality to be temporarily lifted under specific circumstances so that confidential patient information can be transferred without the discloser being in breach of the common law duty of confidentiality
Senior Information Risk Owner (SIRO)	An Executive Director or member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk policy.
Social Prescribing	Social Prescribing describes circumstances where GPs, nurses and other primary care professionals refer people to a range of local, non-medical services. It is sometimes known as 'community referral'
Special Category Personal Data	Data about an individual's racial or ethnic origin; political opinion; religious or philosophical beliefs; trade union membership; sex life or sexual orientation; health, including genetic and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see General Data Protection Regulation Article 10)
Subject Access Request	The General Data Protection Regulation gives individuals the right to have access to, and request a copy of, information about themselves. This is known as a Subject Access Request
Supplier due diligence	Supplier due diligence is the process of carrying out research to ensure that a supplier can meet the required standards before entering into a contract
Special Category Personal Data (Sensitive Personal Data)	The General Data Protection Regulation refers to sensitive personal data as "special categories of personal data" (Article 9 – see glossary) Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10 – see glossary)