

***Information Governance Approval Process for  
Research & Development (R&D)***

**Author(s):** Information Governance

**Owner:** Filip Horvat

**Version No:** 1.2

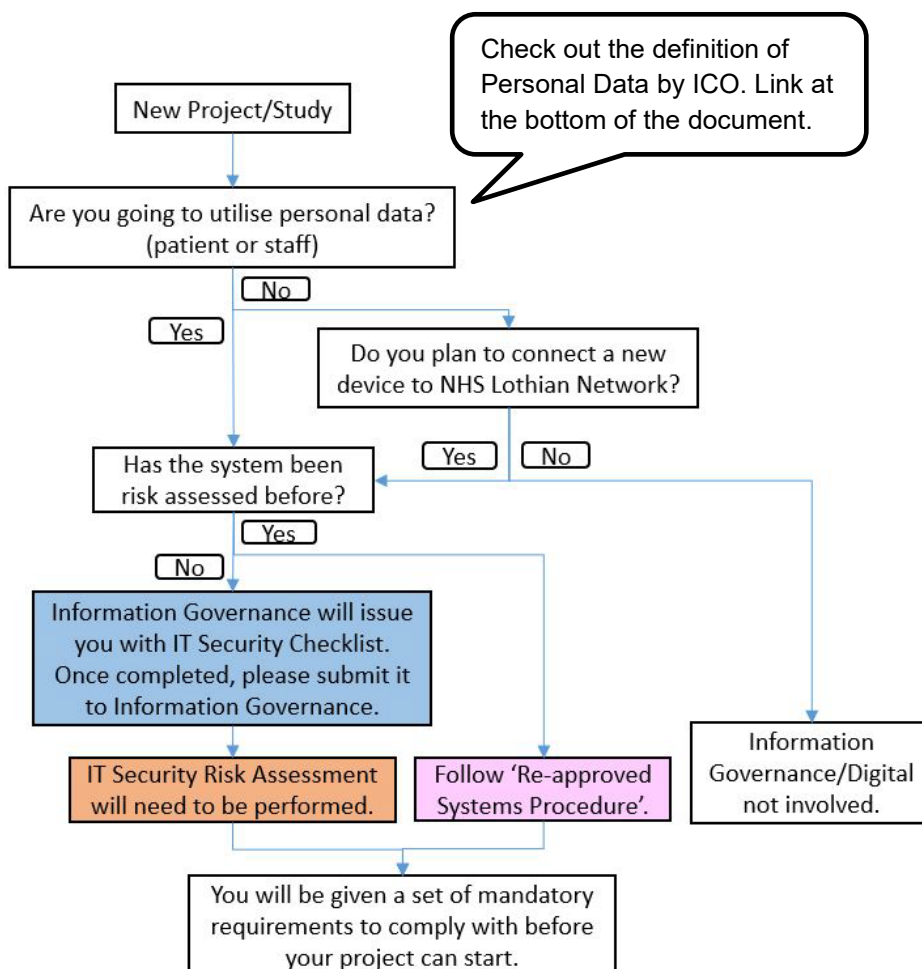
**Status :** Live Version

**Release Date:** 23/02/2021

### Welcome to NHS Lothian Information Governance approval process.

The purpose of this process is to ensure that your research project complies with NHS Lothian internal requirements for Data Protection and Information Governance. This is a process designed to ensure that confidential data are handled safely.

Please follow the flowchart and have a look at the definitions of terms below the flowchart to help you understand each step. To approve your study, we may need to perform an IT Security Risk Assessment or in some cases, confirm that nothing has changed in the system since the last time we performed risk assessment.



### Key Terms:

**IT Security Checklist** – The NHS Lothian Information Governance team will issue the local Investigator and/or the Sponsor/Sponsor Representative with the current version of the NHS Lothian IT Security Checklist. We use this document to gather information about the given system we are required to risk assess (this could be an infrastructure used to host a web-based platform, software solution to be used for

gathering and processing of data, hardware issued to staff/study subjects, etc.). We can provide support to ensure all relevant sections of the checklist are complete to process the risk assessment as quickly as possible.

You may need to forward the IT checklist to a technical department managing the system being risk assessed. It is often necessary to get a level of detail that is only available from technical teams.

**IT Security Risk Assessment** – A completed NHS Lothian IT Security Checklist will be used to perform an IT Security Risk Assessment. The information provided in the IT Security Checklist will highlight any potential risks within the project. These will be documented in the IT Security Risk Assessment, together with mandatory requirements/recommendations for eliminating, reducing and/or mitigating the possible risks highlighted. A project cannot start until we have confirmation that all requirements highlighted in the Risk Assessment have been addressed.

**Re-approved Systems Procedure** - In the case where a system has been used before within NHS Lothian, Information Governance will issue you with Re-approved System Record containing basic information about the system gathered during the last IT Security Risk assessment. Please confirm if the Re-approved System Record is accurate for how the system will be used for your study. You can do this by forwarding the document on to the company/service in question and asking them to confirm compliance. The document will also need to be signed by the staff member requesting the service. Once returned to Information Governance, we will notify you of any new potential risks within the project and recommend possible mitigating techniques and/or requirements. A project cannot start until all requirements have been addressed.

### **Frequently Asked Questions (FAQs):**

#### **- Why is NHS Lothian Information Governance review required for my project?**

Each individual Health Board has responsibility for ensuring that their patient data are handled securely. Some Health Boards may decide to do a risk assessment before participating in a project and some may not. This is up to each Health Board's own discretion. You are receiving this document because our Health Board has determined that we need more information on how patient data will be managed within your project.

#### **- I'm not sure how to fill in the IT security checklist. How can I move forward?**

Your first point of call is the Information Security Project Manager ([gavin.singleton@nhslothian.scot.nhs.uk](mailto:gavin.singleton@nhslothian.scot.nhs.uk)). We can explain which parts of the checklist are relevant to the system you wish to use, and who to speak to within your organisation or a contracted organisation to source the required information. The checklist may need to be filled in by technical team supporting your specific technical data handling solution. Our Information Security Project Manager will be happy to help you with establishing contact with external technical teams and communicating with them directly.

#### **- I'm not collecting any identifiable data, why do I need Information Governance review?**

If you feel like your project has been flagged up to Information Governance incorrectly, please speak to our Information Security Project Manager ([gavin.singleton@nhslothian.scot.nhs.uk](mailto:gavin.singleton@nhslothian.scot.nhs.uk)). It may be that due to the volume or level of detail of data you are collecting, it has been determined that Risk Assessment is required. Alternatively, if you

## NHS Lothian Information Governance approval process

---

are using a new system that will interact with the NHS Lothian network, an IT Security Risk Assessment will be required.

### - Do I need to complete DPIA (Data Protection Impact Assessment)?

During the initial review of your project, the NHS Lothian R&D team will determine whether the design of your project and how personal identifiable data will be processed complies with the NHSL R&D Generic DPIA and local policies and procedures. Where compliance in all these areas is confirmed by R&D, a study specific DPIA is not required. If it is determined that our R&D Generic DPIA does not cover your project in its entirety, R&D team will direct you to Information Governance to determine if a study specific DPIA is required. If available, we will request and can accept an external Sponsors DPIA or we can assist you in completing our NHS Lothian DPIA form.

### **Useful Links:**

For **definition of Personal Data by ICO**, follow this link:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>

For general information about DPIA, please visit <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

For any Information Governance/IT Security queries relating to R&D, you can contact [gavin.singleton@nhslothian.scot.nhs.uk](mailto:gavin.singleton@nhslothian.scot.nhs.uk).