## APPENDIX 7 – CHECKLIST FOR ENSURING INFORMATION GOVERNANCE COMPLIANCE IN THIRD PARTY CONTRACTS

This checklist must be used to sign-off contracts where third parties will have an interface with patients or staff and/or their Personal Confidential Data as having appropriate Information Governance (IG) clauses included.

|  |  |  |
| --- | --- | --- |
| **Required contractual clause** | **Met (Y/N)** | **Comments** |
| The Data Processor ensures the confidentiality of the data being processed. |  |  |
| The Data Processor ensures the technical and organisation security of the data being processed (i.e. Information Security of both paper and digital records), by use of, for example, encryption and pseudonymisation, as well as contractually-agreed backup, restore and recovery processes. |  |  |
| The Data Processor ensures responds to and / or appropriately supports Subject Access Requests within a predefined timescale, so as to allow the Data Controller to respond to the requestor within the month timescale. |  |  |
| The Data Processor ensures will appropriately inform the Data Controller of any Data Breaches (including IG, Information Security, Cyber Security and other related breaches) at the earliest opportunity and no later than 24 hours from becoming aware of the data breach to enable the Data Controller to meet its 72 hours reporting obligation. |  |  |
| The Data Processor ensures will cooperate with the Data Controller in informing Data Subjects if their data has been breached. |  |  |
| The Data Processor ensures will cooperate with any third party incident responders appointed by the Data Controller, national CareCERTs (if health and social carebodies) and law enforcement agencies through the incident management lifecycle. |  |  |
| The Data Processor ensures will fully engage with both Privacy by Design, including Data Protection Impact Assessment, processes when developing new and / or significantly updating existing information systems (paper or digital). |  |  |
| The Data Processor will return all Personal Data to the Data Controller at the end of the provision of services and only delete any copies upon instruction by the Data Controller (having first confirmed that data integrity has been maintained in the transfer or that the data are not required as per retention schedule). |  |  |
| The Data Processor will allow the Data Controller’s preferred penetration testing organisation to actively scan infrastructure hosting digital information for vulnerabilities and to exploit these for the purposes of evidence to the Data Controller and Data Processor. |  |  |

|  |
| --- |
| **Freedom of Information** |
| Duty to disclose (or to support disclosure if a non-public body). |  |  |
| Any exemptions to disclosure provisions. |  |  |
| Responsibility for FOI applications. |  |  |

If the NHS Standard Contract or NHS Terms and Conditions of Contract are used, it is not necessary to complete this checklist, as it incorporates appropriate Information Governance assurance clauses.

## It is the joint responsibility of the Commissioning / Procurement Team and the owning Manager of the contract to ensure this Checklist is completed and held locally.

|  |  |
| --- | --- |
| **Staff member completing form** |  |
| **Staff member signing-off compliance** |  |
| **Details of contract being reviewed** |  |

**All of the following requirements must be met. Answering ‘No’ to any would invalidate the contract from an IG perspective.**

|  |  |  |
| --- | --- | --- |
| **Required contractual clause** | **Met (Y/N)** | **Comments** |
| **Data Protection and Cyber / Information Security** |
| The Data Processor may only engage another processor with specific written authorisation of the Data Controller. |  |  |
| The Data Processor ensures that if they engage another Data Processor for carrying out specific processing activities on behalf of the Data Controller, they ensure the same Data Protection obligations are imposed on them. |  |  |
| The following are defined:* Subject-matter and duration of the processing.
* Nature and purpose of the processing.
* Type of Personal Data.
* Categories of Data Subjects.
* Location of primary data hosting and backup arrangements.
* Obligations and rights of the Data Controller.
 |  |  |
| The Data Processor will only process Personal Data on documented instructions from the Data Controller. |  |  |
| The Data Processor will only transfer Personal Data to a third country or international organisation where there are appropriate safeguards and only if Data Subject rights are legally enforceable there; typically, this means an approved third country with an adequacy decision by a Supervisory Authority, Binding Corporate Rules, or the use of model contract clauses. |  |  |

|  |  |  |
| --- | --- | --- |
| **Required contractual clause** | **Met (Y/N)** | **Comments** |
| **General** |
| Penalties for breach of IG clauses are detailed. |  |  |
| Provisions to indemnify the Trust against breaches by the third party are outlined. |  |  |
| Responsibilities for costs, e.g. for Information Security audit, Subject Access Requests and FOI etc. |  |  |
| The Data Processor will allow Data Protection and related compliance audits of the service provided (without notice where possible or at 24 hours’ notice). |  |  |

**I confirm all IG requirements for this contract are met:**

|  |  |
| --- | --- |
| **Signed (or email embedded)** |  |
| **Name** |  |
| **Designation** |  |
| **Date** |  |