Appendix 4 - Key terms to be included in any contract for level 1 and above information sharing/access with a third party supplier

1. **Information Governance Key Contractual Terms:**
    - Defines who is acting as a 'Data Controller' and who is acting as a 'Data Processor' as outlined in the Data Protection Act /General Data Protection Regulations 2016 or any subsequent legislation to the same effect
    - Compliance with the Data Protection Act /General Data Protection Regulations 2016 or any subsequent legislation to the same effect;
    - Protection of Personal Data;
    - In what circumstances Personal Data can be used by the third party supplier to deliver the agreement;
    - Requirement for the third party supplier to keep the data for no longer than has been agreed with the Health Board;
    - Requirement for the third party to seek permission from the Health Board prior to it entering any new agreement to share the data with any other organisation or third party.
    - Confidentiality including the requirement for all staff to have appropriate confidentiality clauses in their employment contract.
    - Notification to the Health Board of any information security incident as soon as possible and, at the least, within 24 hours.
    - Agreement to assist the Health Board in responding to FOI requests and requests from individuals to access their personal data (in relation to S.7 of the Data Protection Act) in relation to any information held as part of the agreement.
    - Ensure that the third party supplier does not allow information to be transferred outside of the European Economic Area without the explicit consent of the Health Board.

2. **Security Key Contractual Terms:**
    - Requirement to have appropriate Security Policies in place and ensure that all employees comply with these requirements.
    - Notification of the Health Board in relation to any changes to the Security Policy.
    - Sets out the security standards that the third party must meet as a minimum:
      - ISO 27001 (for all level 2 and above agreements)
      - Cyber Essentials (for all level 2 and above agreements)
      - Cyber Essential Plus (for all level 3 agreements)
    - Sets out any specific security requirements around how systems, software or paper records are stored and used.

- Sets out the requirement to have in place a tested Business Continuity and Disaster Recovery Plan.
- Agreement to allow the Health Board access to any buildings, systems etc holding data as part of the agreement for its own auditing purposes so long as reasonable notice is given.
- Ensuring appropriate controls are in place around the information held as part of the agreement to ensure only authorised personnel have access.
- Sets out the principles of an exit strategy and the transfer and/or secure destruction arrangements for any information held at the end of or, upon termination of the agreement.