2.11.2	Data Protection Assessment		
	Question	**Help Text**	**Guidance**
2.11.2.10	*Provide a general description of the security measures in place to keep project data secure for each system, platform and application you will use for access, storage, and transfer, including but not limited to multi factor authentication, use of passwords, use of VPN, device encryption, vendor ISO certification, anti-virus used, use of secure file transfers such as HEAnet, and detail on how data is backed up etc.*	Please detail all technical and organisational security measures you will put in place to safeguard electronic and paper-based personal data. This should include access controls, physical security controls ,technical security measures (including but not limited to multi-factor authentication, use of passwords, use of VPN, encryption, vendor ISO certification, anti-virus. etc. See Guidance - please review carefully before answering.	**List each system involved** List each system involved and what measures are in place for each including but not limited to; multi factor authentication, use of VPN, encryption, vendor ISO certification, anti-virus used, use of secure file transfers such as HEAnet etc. **Detail the following for each system processing the personal data** 1. Does the system processing the personal information have access controls? (E.g. role-based, location-based, time-based) • Indicate how events are logged and how long this log is kept. • If role-based controls, please provide a table outlining roles and responsibilities. • If location based, how is physical access controlled? 2. If the data is transferred from one system to another, how is this accomplished? • Laptop (portable device); Email; FileShare. • Third party services (where is the service located?). • Removable media - USB/removable hard drive. • Printed/paper copies (how documents are printed, stored, destroyed when no longer required etc.). 3.Other (describe). • If data is on physical devices/paper, how is it transferred (e.g. registered post, courier)? Provide detail. 4. Is data encrypted in transit? If yes, please provide encryption method - e.g., 128-bit, 256-bit, Full disk, file level, VPN etc. 5. Is the data encrypted at rest? If yes – please provide level of encryption - e.g. 128-bit, 256-bit, Full disk File level, VPN etc.