HYWEL DDA UNIVERSITY HEALTH BOARD

Third Party Supplier Security Policy

Policy information

Policy number: 279

Classification: Corporate

Supersedes: All previous policies

Version number: 3

Date of Equality Impact Assessment: 14.10.2024

Approval information

Approved by: Sustainable Resources Committee

Date of approval: 22.10.2024

Date made active: 23.10.2024

Review date: 22.10.2027

Summary of document:
The purpose of this policy is to ensure that all contracts and agreements between the Health Board and third-party suppliers have acceptable levels of information security and information governance processes to ensure that personal and sensitive data is protected and managed in line with statutory and good practice requirements.

Scope:
This policy applies to all staff and service areas across the Health Board. It applies to all agreements and contracts entered into with a third party (any organisation outside of the Hywel Dda Health Board) that involves (or may involve in the future) direct or indirect access to patient, staff or other sensitive
information.

To be read in conjunction with:
172 - Confidentiality Policy ‘opens in a new tab’
347 - Corporate Records Management Policy ‘opens in a new tab’
836 - All Wales Information Governance Policy ‘opens in a new tab’

837 - All Wales Information Security Policy ‘opens in a new tab’
238 - Information Governance Framework ‘opens in a new tab’
320 - Acceptable use of Digital Services Policy ‘opens in a new tab’

Patient information:
Include links to Patient Information Library

Owning group:
Information Governance Sub-Committee
24/07/2024

Executive Director job title:
Director of Finance

Reviews and updates:
1 – new policy May 012
2 – updated 26.6.2018
3 – Full review 22.10.2024

Keywords
Third Party Security, procurement

Glossary of terms
Data Protection Legislation:
NIS Regulations: The Security of Network and Information Systems Regulations 2018
Special Category Data:

Keypoints:
This policy outlines the process that must be followed prior to any contracts and/or agreements being entered into with a third party by the Health Board. It will provide assurance to the Health Board, our staff and patients that every agreement or contract entered into meets appropriate technical and security measures to protect personal and/or confidential information.

Contents

HYWEL DDA UNIVERSITY HEALTH BOARD

Introduction

In order to provide effective health services, the Health Board will need to enter into contracts and agreements with outside organisations. For the purposes of this policy, these organisations will be referred to as 'third party suppliers'. These third party suppliers may be primary or sub- contractors or relate to any other party (including individuals regular sole traders) that the Health Board enters into an agreement with to provide services to our patients.

Information and information systems are vital assets of the Health Board. It is essential that the organisation has the appropriate technical and security measures in place to protect this information. This requirement becomes increasingly important in the case of patient, staff and other sensitive information and where there is a requirement to share this information with third parties who are delivering services on behalf of the Health Board.

This policy outlines the process that must be followed prior to any contracts and/or agreements being entered into with a third party by the Health Board. It will provide assurance to the Health Board, our staff and patients that every agreement or contract entered into meets appropriate technical and security measures to protect personal and/or confidential information.

Policy Statement

The Health Board recognises its responsibility to process its personal information correctly and in-line with all legal, regulatory and internal policy requirements.

In addition to its statutory requirements, the Health Board recognises the importance of protecting patient and staff information to ensure the delivery of the best possible patient care.

Scope

This policy applies to all employees, volunteers or other individuals working on behalf of the Health Board who are responsible for entering into any agreement or contract (both local or national) with third parties that involves the third-party having access to or receiving Health Board information.

This policy covers all aspects of personal information within the Health Board, including but not limited to:

- Patient/client/service user information.
- Personnel and staff information.
- Sensitive corporate information.

This policy applies to both electronic and hard copy/physical copies of information.

This policy applies to all instances where information is shared with a third-party supplier and their employees or any party within their supply chain and where the third party may have access to the Health Board's systems or networks or to physical information held on and off-site of Health Board premises.

This policy also applies to instances where a third party, their employees and any party within their supply chain may have indirect access to information i.e. staff/cleaners accessing rooms that may contain patient data, individuals transporting patient information etc.

HYWEL DDA UNIVERSITY HEALTH BOARD

Aim

This policy will ensure that the Health Board complies with its statutory duties laid out in the Data Protection Act 2018 /UK General Data Protection Regulations 2016 or any subsequent legislation to the same effect, the Human Rights Act 1998 and with the common law duty of confidentiality.

It will ensure that all third-party organisations who enter into an agreement or contract with the Health Board are clear about the Health Board's expectations in terms of information security and confidentiality.

It will ensure that both the Health Board and any organisation acting as a data processor for the Health Board will have the relevant technical and security measures in place to meet data protection legislation, privacy and Cyber Security requirements.

The correct application of this policy will ensure that the Health Board is compliant with its legislative responsibilities, reduce the risk of an information security breach taking place and provide assurance to our staff and patients that information assets are being properly managed.

Objectives

Ensuring that staff and third parties understand their responsibilities for information security, data protection, confidentiality and privacy will meet the following objectives:

- Protect and prevent personal or confidential information from being lost, stolen or intercepted by unauthorised persons.
- Reduce the risk of an information security breach from taking place.
- Maintain patient and staff trust in the Health Board and any third parties they commission or enter into agreements with, that their personal information is being managed safely and appropriately.
- Ensure that access to information is maintained by preventing information from being lost or stolen or sent to the wrong individual or location.
- Ensure the Health Board is meeting its legal and ethical duties in relation to maintaining confidentiality in line with data protection legislation, the common law duty of confidentiality, the Human Rights Act and other legislative requirements.
- Ensure the Health Board is meeting appropriate security requirements as laid out in ISO27001 standards and the Welsh Health Circular (2017) 025 'opens in a new tab'.
- Ensure the Health Board is meeting the confidentiality requirements as laid out in in the UK Network and Information Systems Regulations 2018.

Process to be followed

Before commencing the tender process or entering into any agreement with a third-party supplier.

Overview of main tasks to be completed

There are three main tasks that must be completed by the staff member responsible **prior to commencing the tender process** or entering into any formal agreement with a third party supplier:

- **Task 1:** Complete the Third Party Supplier Screening Document and forward to your link in procurement (If procurement are not involved in setting up the agreement, the staff member

will then also need to complete page one of the Third Party Supplier Screening Document and send it off to the third party supplier for completion (See Appendix 1a for process summary and Appendix 2 and Appendix 3 for copies of the documents).

- **Task 2:** Carry out a Data Protection Impact Assessment if required – See Appendix 1b for process summary.

- **Task 3:** Checking appropriate contract/agreement arrangements are in place – See Appendix 1c for process summary and Appendix 3 for a list of requirements.

  Assistance is available from the Information Governance Team if required in completing any of the above tasks: Information.Governance.HDD@wales.nhs.uk

Task 1: Completing the Third-Party Supplier Screening Document

The Third-Party Supplier Screening Document (Appendix 2) will ask the responsible staff member to indicate the level of information being shared/accessed with the third party supplier and is split into the following four areas:

No personal/sensitive information shared (Level 0 access to information)

- The supplier, or any party within their supply chain, does not store, process or have access to patient, staff or other sensitive personal information, nor access to sensitive corporate information.
- The supplier, or any party within their supply chain, does not have any form of networked/ electronic communication or access to devices on the NHS Wales network, including connecting into networks/devices when their staff are on NHS sites.

  NB: the sorts of contracts this will apply to are likely to be those covering commodity purchases or standard service provisions (e.g. office supplies or the disposal of non- sensitive waste).

Low level access to information (Level 1 access to information)

- The supplier, or any party within their supply chain, could have access to very limited amounts of patient, staff or other special category personal data/information which is stored on the NHS network, or very limited access to sensitive corporate information. No such information will be stored by the supplier for any party within the supply chain in electronic or paper form. i.e. the supplier will not take away or store any information off site or outside of the Health Board's network or systems.
- The supplier, or any party within their supply chain, require ad-hoc infrequent access to devices which are connected to the NHS Wales network, or the network itself, which would be achieved through attending sites and connecting directly into the equipment.
- The supplier, or any party within their supply chain, could have access to very limited amounts of patient, staff or other special category personal information which is stored on the NHS network, or very limited access to sensitive corporate information. No such information will be stored by the supplier or any party within the supply chain.
- The supplier may be at a Health Board site where their employees may have indirect access to physical patient, staff or other confidential information. They are likely to be accompanied by a Health Board employee at all times when on site.

NB: The sorts of contracts this will apply to could include maintainers of building management systems, printer maintenance companies, suppliers of specialist non-clinical software, cleaning contracts, maintenance contracts etc.

Moderate level/risk access to information (Level 2 access to information)

- The supplier, or a party within their supply chain, have access to greater volumes of, or more sensitive, personal data relating to staff or patients, or access to special category information. This information could be stored and processed on the NHS systems/network or by the supplier, or a party within their supply chain.
- The supplier, or a party within their supply chain will only store information within UK.
- The supplier, or a party within their supply chain, may require frequent access to devices which are connected to the NHS Wales network, or the network itself, which is either achieved through attending site and connecting directly, or via an authorised remote access mechanism.
- The supplier, or a party within their supply chain, will have direct access to physical copies of sensitive, personal data relating to staff or patients, or sensitive corporate information. Physical copies of the information will not be removed by the supplier from a Health Board site.

NB: The sort of contracts this will apply to are organisations storing or processing smaller amounts of information on behalf of the Health Board that does not contain special category of personal data, e.g. a supplier processing name, address and contact details of a staff member or basic demographic information.

High level/risk access to information (Level 3 access to information)

- The supplier, or a party within their supply chain are responsible for supporting key clinical capability within the Health Board. They will be handling or have access to bulk/large amounts of special category of personal information relating to staff or patients or, highly confidential corporate information. This information could be stored and processed on the NHS systems/networks or by the supplier on their own systems/network, or by a party within their supply chain.
- The supplier, or a party within their supply chain will only store information within UK.
- The supplier, or a party within their supply chain, may require frequent access to devices which are connected to the NHS Wales network, or the network itself, which is either achieved through attending site and connecting directly, or via an authorised remote access mechanism.
- The supplier, or a party within their supply chain, will have direct and unsupervised access to bulk/large amounts of physical copies of special category of Personal data, personal data relating to staff or patients, or sensitive corporate information.
- Physical copies of patient, staff or sensitive corporate information may be removed by the supplier from a Health Board site or stored by the supplier away from a Health Board site.

NB: The sort of contracts this will apply to are organisations storing or processing large/bulk amounts of information on behalf of the Health Board that contains special category of personal data e.g. a supplier processing health information, ethnicity, religious beliefs, disability information etc.

Once the responsible staff member has confirmed the level of information to be shared or accessed using the above criteria, they can complete the Third Party Supplier Security Screening Document (Appendix 2). The responsible staff member should sign and date the document and forward a copy to their link in the procurement department.

NB: If the individual responsible is not going through procurement for the purposes of the contract or agreement they must follow below steps themselves.

The Procurement lead (or responsible individual) will complete Part One of the 'Third Party Supplier Security Questionnaire' (Appendix 3) with the appropriate level using the screening document outlined above. The Procurement lead (or responsible individual) will send a copy of the 'Third party Supplier Security Questionnaire' to all suppliers involved in the tender and ask that it is completed as part of their tender return.

The response from the supplier to the 'Third Party Supplier Security Questionnaire' will be returned to the responsible individual and to the Procurement Team. The responsible individual will need to review this at the same time as the tender awarding process to ensure that the relevant security standards are met for their chosen supplier. This can be done with the assistance of the Information Governance Team if required.

The agreement is then signed off and agreed by the Information Asset Owner or Assistant Director (or similar staff level) and a copy sent to the Information Governance Team for their records.

If the response from the supplier meets the required security standards, then the responsible individual can go ahead and enter into a formal contract or agreement with their chosen supplier.

If the response does not meet the required security standards then the responsibly staff member will need to seek advice from the Information Governance Team in terms of whether the identified risk can be accepted. The procurement process will be put on-hold until this process has been completed. The Information Governance Team can be contacted at the following address: Information.Governance.HDD@wales.nhs.uk
process

Task 2: Carrying out a Privacy Impact Assessment if required

For any agreements entered into that meet a Level 1 and above, the need for a Data Protection Impact Assessment (DPIA) must be considered at the earliest opportunity before the tender process commences if any of the following apply:

- If the new contract/agreement will involve the collection of new information about individuals that is currently not being collected by the service area.
- If the new contract/agreement will involve using information collected about individuals for a different purpose than it is currently being used for.
- If the new contract/agreement will involve sharing information about individuals with organisations or people who have not had access to it before.
- If the new contract/agreement involves using technology that may be perceived as being privacy intrusive .e.g CCTV, biometric scanning etc.
- If the new contract/agreement involves making decisions about people that will have a significant impact on their lives.
- If the new contract/agreement will involve making automated decisions about people.
- If the new contract/agreement involves the processing of particularly sensitive information about people e.g. personnel records, health records, criminal records, child health records etc.
- If the new contract/agreement will involve contacting people in a way then may find

intrusive e.g. cold calling at their home phone number or address, sending sensitive information to a home address that could be seem by other household members etc.

A Data Protection Impact Assessment is a tool that works through a number of questions about a new project, system or policy. It makes sure any proposal will be compliant with any privacy, and Information Governance requirements and that these are built into the project or system planning stage.

It allows the Health Board to build any specific requirements into the tender process or agree any requirements with a new supplier prior to entering into a formal agreement. This makes sure that money isn't wasted on purchasing new systems or services that are not compliant with our legal obligations and which then later have to be changed or added to, often at an additional cost to the organisation.

If the responsible individual considers that the new contract/agreement is likely to meet any of the above criteria, then they should contact the Information Governance Team for assistance in completing a Data Protection Impact Assessment prior to going out to tender or entering into any formal agreement with a third-party supplier.

Task 3 - Checking appropriate contract/agreement arrangements are in place

A formal contract between Hywel Dda University Health Board and the third-party supplier shall exist to protect both parties. The contract must clearly define the types of information exchanged and the purpose for doing so.

For all supplier agreements and contracts that score a level 1 and above, any agreement or contract must specify the appropriate confidentiality, information and cyber security requirements as laid out in Appendix 4 of this policy. This can be included as part of the contract itself or as a separate confidentiality or Data Processing Agreement which may be required before the main contract is negotiated.

All contracts must be submitted to the Procurement Team to ensure for accurate content, language and presentation. All confidentiality or Data Processing Agreements must be submitted to the Information Governance Team to ensure they meet the required needs of the proposed agreement.

For any individual entering into an agreement with a third party supplier outside of the procurement process where personal information will be shared at a level 1 or above, they must ensure that the agreement includes as a minimum the requirements laid out in Appendix 4.

Data Processors and Data Processing Agreements

If the responsible individual is entering into an agreement with another organisation who is acting as a data processor, then, in addition to any contract, a Data Processing Agreement must be signed and agreed by the third party supplier.

A third-party supplier will usually be acting as a Data Processor for the Health Board if they meet the following criteria:

- The Health Board keeps control over 'why' and 'how' the information is used by the supplier. The supplier simply follows the directions from the Health Board about how the information is managed and for what purposes.
- The Health Board keeps control over telling the supplier what information is collected and stored. The supplier follows these instructions.

- The Health Board advises the supplier how long the information is stored for. The supplier follows these instructions.
- The supplier can decide the technical aspects of the agreement i.e. what IT systems it uses, the detail of any security measures it has in place, the means used to transfer information from one organisation to another, the means used to securely delete or dispose of information.

It is important for the responsible staff member to be clear when a third-party supplier is acting as a data processor as, in these cases, the Health Board has a legal responsibility to make sure the supplier has appropriate arrangements in place to safeguard any information they are holding or have access to.

It is therefore very important that proper contract and Data Processing Agreements are in place to protect the Health Board and its information in these cases. The Information Governance Team have sample Data Processing Agreements that can be used for these purposes.

If individuals are unsure as to whether they are entering into an agreement with a third party who will be acting as a Data Processor, then further advice and guidance can be given by the Information Governance Team.

Roles and Responsibilities

Chief Executive & Hywel Dda University Health Board:
The Chief Executive and Hywel Dda University Health Board have a duty to ensure that the requirements of current data protection legislation are upheld and the Chief Executive has overall responsibility for implementation of this policy.

Executive Directors:
Executive Directors are responsible for the overall management of information risk within their service areas and are responsible for ensuring their staff and managers are aware of this policy.

The Senior Information Risk Owner and Caldicott Guardian:
The Senior Information Risk Owner and Caldicott Guardian are responsible for managing information risk and the safe and ethical use of information across the health board and are responsible for ensuring their staff and managers are aware of this policy.

Information Asset Owners:
Information Asset Owners are responsible for understanding what information is held within their service areas and where contracts and agreements are being entered into with third party suppliers involving the sharing of or access to Health Board information. These arrangements with third party suppliers should be listed on their individual information asset registers.
Information Asset Owners are able to delegate this responsibility to another named individual within their service area, but they must retain overall responsibility for ensuring that this policy is followed when any of their staff enter into a third party contract or agreement.

Information Governance Team:
The Information Governance Team are responsible for disseminating this policy across the Health Board and ensuring it is readily available to all staff. The team are responsible for providing appropriate support and advice to the Information Asset Owners, Service Lead, staff and managers to ensure the policy is understood and adhered to.

Procurement Team
The Procurement Team are responsible for ensuring that the appropriate Third-Party Supplier Security Questionnaire is sent to potential suppliers as part of the procurement process and that any contracts sent via their team meet the minimum requirements as laid out in this document.

Line Managers
Line Managers must ensure that they comply with the requirements of this policy when entering into any new contracts or agreements with third party suppliers. They must ensure that any staff they are responsible for have read and understood this policy and monitor staff compliance in meeting the policy requirements. Line Managers are responsible for reporting the non- compliance of this policy to the Information Governance Team.

All staff
All staff must read, understand and comply with this policy. If a staff member is not clear about any aspect of this policy and its application, they are responsible for raising this with their line manager for further clarification.

References

Data Protection Act 2018
UK General Data Protection Legislation 2016
NIS Regulations 2018
WCH: Guidance on Cyber Security and Information Governance Requirements relating to suppliers and the supply-chain.'

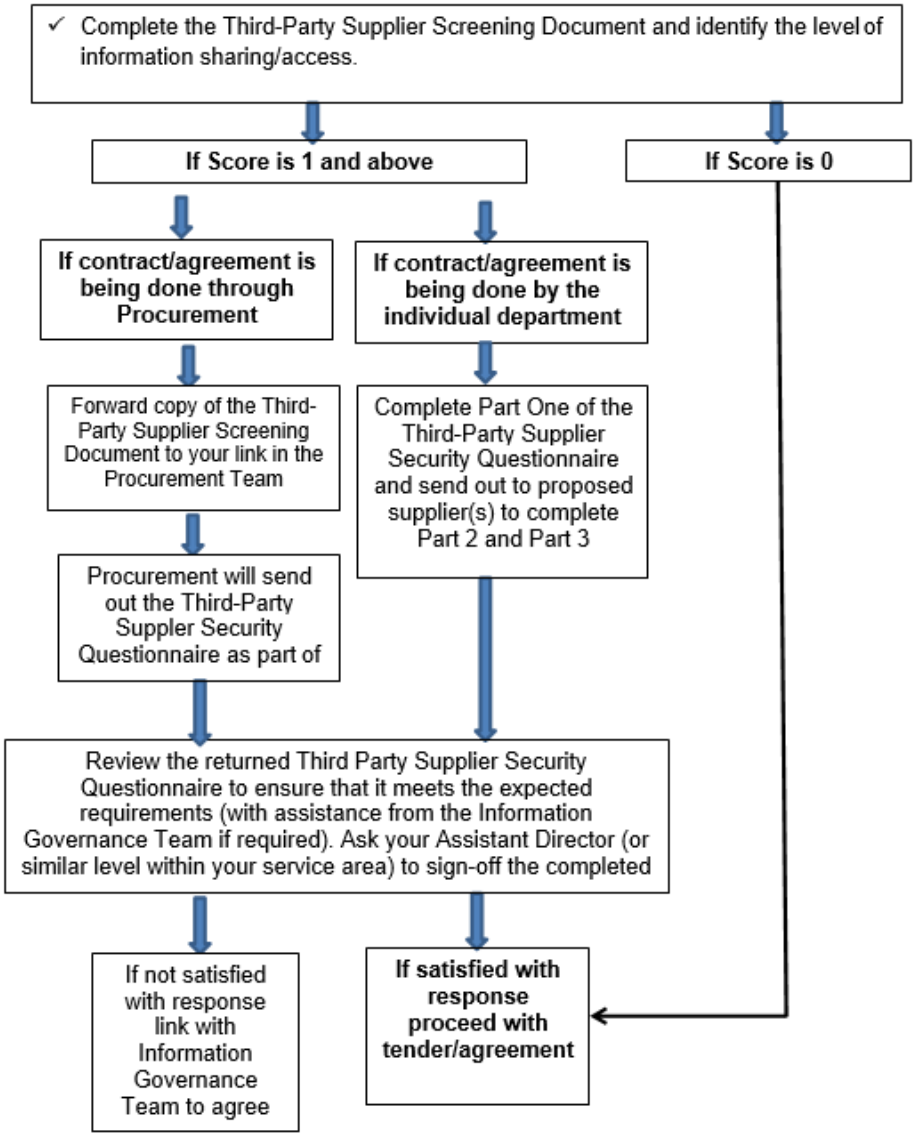
Should you have any queries in relation to this policy please email the Information Governance Team at Information.Governance3@wales.nhs.uk, alternatively, you can contact:
Data Protection Officer (DPO) at: DPO.HDD@wales.nhs.uk,
Senior Information Risk Officer (SIRO) at: SIRO.HDD@wales.nhs.uk
Caldicott Guardian at: CaldicottGuardian.HDD@wales.nhs.uk

HYWEL DDA UNIVERSITY HEALTH BOARD

Appendix 1a – complete the third party supplier screening and third party supplier security questionnaires

Checklist for staff before entering into a third-party supplier agreement or contract

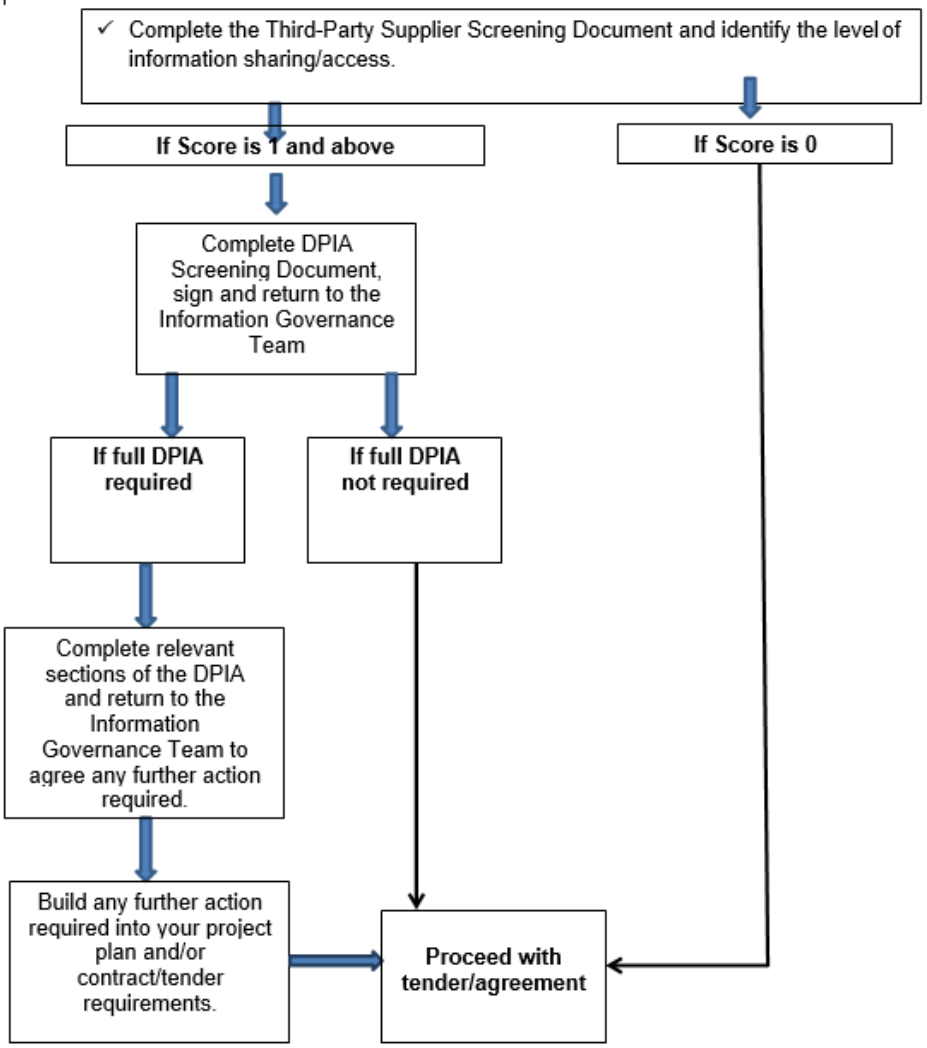
11. Appendix 1a – Task One: Complete the Third-Party Supplier Screening and Third-Party Supplier Security Questionnaires.



Appendix 1b – task 2 carry out a data protection impact assessment if required

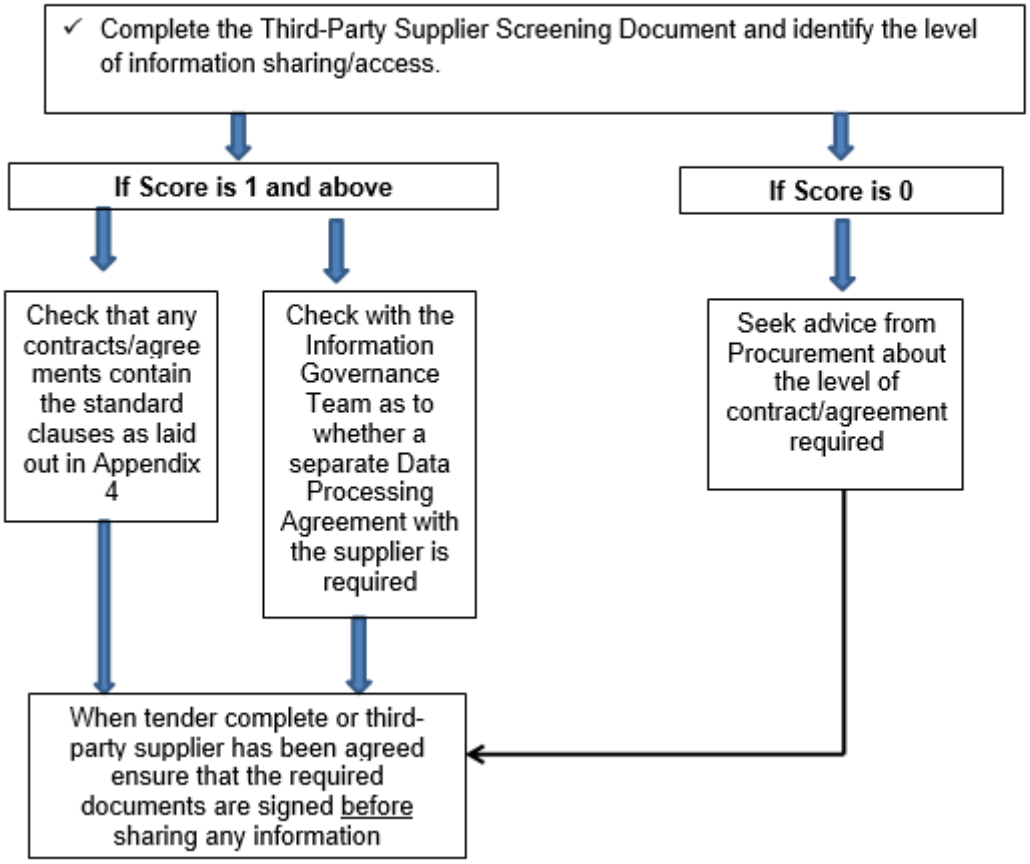
Checklist for staff before entering into a third-party supplier agreement or contract

12. Appendix 1b – Task Two: Carry out a Data Protection Impact Assessment (DPIA) if required



HYWEL DDA UNIVERSITY HEALTH BOARD
Appendix 1c – task three: checking contract/agreement arrangements

Checklist for staff before entering into a third-party supplier agreement or contract
13. Appendix 1c – Task Three: Checking contract/agreement arrangements



HYWEL DDA UNIVERSITY HEALTH BOARD

Appendix 2 Third party supplier screening document

This document will advise you what further action you need to take prior to going out to tender and/or entering into any agreement or contract with a third-party supplier. A 'third party supplier' is any organisation outside of the Hywel Dda University Health Board who we are entering into an agreement with to carry out a service on our behalf.
This document should be completed by the manager responsible for entering into any contract or agreement with a third-party supplier.

To complete this document:

1. Read a description of the type of information you will be sharing as part of your proposed agreement or contract with a third-party supplier in Section One.
2. Tick the corresponding security level that best matches the type of information you will be sharing in Section Two.
3. Carry out the corresponding further action for the security level you have chosen.
4. Return a signed copy of this document to your link within the Procurement Team (or, to the Information Governance Team if you are not using procurement for your contract/agreement).

Section One:

Description of Information Shared	Security Level
No personal/sensitive information shared: • The supplier, or any party within their supply chain, does not store, process or have access to patient, staff or other sensitive personal information, nor access to sensitive corporate information. • The supplier, or any party within their supply chain, does not have any form of networked/ electronic communication or access to devices on the NHS Wales network, including connecting into networks/devices when their staff are on NHS sites. **NB**: the sorts of contracts this will apply to are likely to be those covering commodity purchases or standard service provisions (e.g. office supplies or the disposal of non- sensitive waste).	**Level 0**

Low level/risk access to information • The supplier, or any party within their supply chain, could have access to very limited amounts of patient, staff or other special category personal data/information which is stored on the NHS network, or very limited access to sensitive corporate information. No such information will be stored by the supplier for any party within the supply chain in electronic or paper form. i.e. the supplier will not take away or store any information off site or outside of the Health Board's network or systems. • The supplier, or any party within their supply chain, require ad-hoc infrequent access to devices which are connected to the NHS Wales network, or the network itself, which would be achieved through attending sites and connecting directly into the equipment. • The supplier, or any party within their supply chain, could have access to very limited amounts of patient, staff or other special category personal information which is stored on the NHS network, or very limited access to sensitive corporate information. No such information will be stored by the supplier or any party within the supply chain. • The supplier may be at a Health Board site where their employees may have indirect access to physical patient, staff or other confidential information. They are likely to be accompanied by a Health Board employee at all times when on site. **NB**: The sorts of contracts this will apply to could include maintainers of building management systems, printer maintenance companies, suppliers of specialist non-clinical software, cleaning contracts, maintenance contracts etc.	**Level 1**
Moderate level/risk access to information • The supplier, or a party within their supply chain, have access to greater volumes of, or more sensitive, personal data relating to staff or patients, or access to special category information. This information could be stored and processed on the NHS systems/network or by the supplier, or a party within their supply chain. • The supplier, or a party within their supply chain will only store information within UK. • The supplier, or a party within their supply chain, may require frequent access to devices which are connected to the NHS Wales network, or the network itself, which is either achieved through attending site and connecting directly, or via an authorised remote access mechanism. • The supplier, or a party within their supply chain, will have direct access to physical copies of sensitive, personal data relating to staff or patients, or sensitive corporate information. Physical copies of the information will not be removed by the supplier from a Health Board site. **NB:** The sort of contracts this will apply to are organisations storing or processing smaller amounts of information on behalf of the Health Board that does not contain special category of personal data, e.g. a supplier processing name, address and contact details of a staff member or basic demographic information.	**Level 2**

High level/risk access to information	Level 3
• The supplier, or a party within their supply chain are responsible for supporting key clinical capability within the Health Board. They will be handling or have access to bulk/large amounts of special category of personal information relating to staff or patients or, highly confidential corporate information. This information could be stored and processed on the NHS systems/networks or by the supplier on their own systems/network, or by a party within their supply chain. • The supplier, or a party within their supply chain will only store information within UK. • The supplier, or a party within their supply chain, may require frequent access to devices which are connected to the NHS Wales network, or the network itself, which is either achieved through attending site and connecting directly, or via an authorised remote access mechanism. • The supplier, or a party within their supply chain, will have direct and unsupervised access to bulk/large amounts of physical copies of special category of Personal data, personal data relating to staff or patients, or sensitive corporate information. • Physical copies of patient, staff or sensitive corporate information may be removed by the supplier from a Health Board site or stored by the supplier away from a Health Board site. **NB:** The sort of contracts this will apply to are organisations storing or processing large/bulk amounts of information on behalf of the Health Board that contains special category of personal data e.g. a supplier processing health information, ethnicity, religious beliefs, disability information etc.	

Section Two:
Tick the level that best matches the type of information you will be sharing as part of your proposed contract or agreement with a third-party supplier:

Level	Tick the most appropriate level that applies using the descriptions above	Further action required
0		**1.** No further action required. **2.** Proceed with your tender process as normal.

1 - 3		**Before commencing the tender process** **1.** Complete a Data Protection Impact Assessment. This must be signed off by the Information Asset Owner or Assistant Director (or similar level of staff) and a copy returned to the Information Governance Team. **2.** Complete Part One of the 'Third Party Supplier Security Questionnaire' available below in Appendix 3 or by contacting the Information Governance Team and return to procurement to send out together with the tender document. **NB:** If you are not going through procurement to enter into a contract or agreement you will need to send the 'Third Party Supplier Security Questionnaire' to the supplier yourself and ask that is returned and completed before entering into any formal agreement. **Before entering into a contract or formal agreement** **3.** Review the response to the Third-Party Supplier Security Questionnaire and check you are satisfied with the response from the supplier (together with the Information Governance Team if required). **4.** Review your completed Data Protection Impact Assessment to assess whether any further work is required (together with the Information Governance Team if required). **5.** Information Asset Owner or Assistant Director (or similar staff level) signs-off the returned Security Questionnaire and a copy is sent to the Information Governance Team. **6.** Proceed with the contract/agreement.

Section three

Please sign below and return a completed copy of this form to your link within the Procurement Team (or, to the Information Governance Team if you are not using procurement for your contract/agreement).

Completed by:
Name:
Job Title:
Signature:

If you need help, advice or support in completing any of these documents then please contact the Information Governance Team: Information.Governance.HDD@wales.nhs.uk

Hywel Dda University Health Board

Third Party Supplier Security Questionnaire

Version No: 2

Authors: IG Team

Approver: IGSC

Date:

Information Governance Team
Hywel Dda University Health Board

Information.Governance@wales.nhs.uk

This document must be completed and signed by any third parties who are entering into an agreement or contract with the Health Board and where they will have access to personal and/or confidential information.

HYWEL DDA UNIVERSITY HEALTH BOARD

Third Party Supplier Security Questionnaire (SSQ)

This SSQ has been issued by the Hywel Dda University Health Board (the Health Board) to serve as a preliminary assessment of the security controls that any third-party supplier has in place prior to entering into any formal agreement with that supplier to access or process any personal or confidential data.
On completion of this document the Health Board will decide whether the third-party organisation in question has the sufficient security controls in place to satisfy our information governance and security requirements.
Any deliberately false statements made will be treated as a breach of contract under this agreement.

Part One

(To be completed by the procurement link or responsible staff member)
Supplier Name & Address:
……
……
……

The supplier has been asked to complete all questions that relate to Level……. of this Assessment Questionnaire *(enter level from Third party supplier screening document e.g. Level 1, 2 or 3).*

Part Two

(To be completed by the Third-Party Supplier)
Please complete the relevant sections below for the Level you have been awarded in the box in Part One above:

Policy Overview

Control Area	Control Question	Supplier response
Security Policies: To be completed for **Level 1,2 and 3**	Does your organisation have documented information security policies? *If yes, please provide copies or a link to your policies with your response to this document.*	
	How often are your security policies reviewed and updated?	
	Who is responsible in your organisation for security policy development and assurance?	
	How do you ensure that all staff and users are aware of your security policies?	
	Do you have a specific information security incidents management policy/procedure and is this compliant with the Data Protection Legislation? *If yes, please provide copies or a link to your policies with your response to this document.*	
Policy Coverage: To be completed for **Level 1, 2 and 3**	Select the security areas which are addressed within your information security policies and standards: ☐ Acceptable use ☐ Remote Access/Wireless ☐ IT Security Incident Response ☐ Data/system classification ☐ Third party connectivity ☐ Physical Security ☐ Network/Perimeter Security ☐ Data Privacy/Confidentiality ☐ Access Control ☐ Encryption Standards ☐ Anti-virus ☐ E-mail/Instant Messaging ☐ Staff confidentiality/security ☐ Clear desk ☐ Removable devices policy	
	What security requirements do you ask for as part of your contracts with any third parties you contract with (if applicable)?	
	Is a complete set of your	

	organisation's policies available for review if required?	

Detailed Security Control Assessment

Organisational Security: To be completed for **Level 2 and 3**	Have security-related job responsibilities, including oversight and accountability been clearly defined and documented within your organisation?	
	Have your security polices, standards and procedures been reviewed by a qualified third party?	
	Do you maintain an inventory of all important information assets held by your organisation and which are clearly associated with a named asset owner?	
	Describe how you monitor access controls to your systems and information.	
Staff/personnel Security: To be completed for **Level 1,2 and 3**	Do all your staff and those of any third parties you contract with have the requirements for confidentiality and compliance with information security/Data Protection laid out in their contract of employment?	
	Do you carry out formal training for all of your staff around confidentiality/information governance/Data Protection/Information Security?	
	Do you have a formal process that outlines the actions that will be taken should a staff member breach any of your information security or related policies?	
	Do you have a dedicated team or individual who are appropriately trained to manage information security incidents?	
	Are all users of your systems required to sign a confidentiality agreement?	
To be completed for **Level 2 and 3**	Do you have a dedicated team or individual who are appropriately trained to manage information security incidents including any cyber attacks/incidents.	
	Do you undertake any additional	

	training for system administrators, developers and other staff with privileged user rights around confidentiality/information governance/Data Protection/Information Security?	
Physical and Environmental Security: To be completed for **Level 2 and 3**	Describe the physical security mechanisms that prevent unauthorised access to your office space, user work stations and server rooms/data centres.	
	Are all critical information assets located in a physically secure area?	
	How do you protect your systems from environmental hazards such as fire, smoke, water etc?	
	How is third party/visitor access granted to your secure locations?	
	Who manages and maintains your data centre? If you use a third-party contractor to maintain your systems, describe the vetting process by which that contractor was selected.	
To be completed for **Level 3**	If you are storing or sharing information (including in any date centres) located outside of the UK, is this information being stored or shared within any of the countries in EEA or countries identified as being on EU Commission's 'list of countries or territories providing adequate protection for the rights and freedoms of data subjects'? *If yes, please advise where the information will be stored.*	
	If you are storing or sharing information outside of UK or outside the EEA or one of the countries listed on the EU Commission's list above, please advise: • where the information will be stored/shared • what controls you have in place to protect that information? *(NB – if a supplier answers 'yes' to this question please refer to the Information Governance Team to ensure that appropriate contract and security arrangements can be checked).*	

System Security: To be completed for **Level 2 and 3**	How do you protect your systems against viruses?	
	Do you carry out regular vulnerability testing against your major systems? If yes, how often do you undertake this testing?	
	How do you prevent your users from installing potentially malicious software?	
	Do you hold certification against the following that has been verified by an appropriate certification body? ☐ *ISO 27001* ☐ *Cyber Essentials*	
To be completed for **Level 3**	Do you hold certification against the following that has been verified by an appropriate certification body? ☐ Cyber Essentials Plus *If yes, please provide evidence of your certification when returning this form*	
Retention schedule and secure destruction: To be completed for **Level 2 and 3**	Do you have a retention policy or schedule that outlines the storage time-scale against all of your information assets?	
	How do you dispose of computer hardware when no longer required?	
	How do you securely dispose of hard and electronic copy data?	
Access controls: To be completed for **Level 2 and 3**	Do you carry out periodic checks to ensure that your users' access rights are up to date and appropriate for their level of responsibility?	
	Do you enable any remote admin capabilities in your servers and network devices? If so, which protocol(s) do you use?	
	Do you audit or monitor system user access to your systems?	
	Are failed log-in attempts recorded and reviewed on a regular basis?	
	What other controls do you have in place to monitor system access?	
Business Continuity: To be completed	Do you have up to date business continuity plans in place for all systems, data centres and networks that will be holding our data as part of	

for **Level 2 and 3**	this agreement? If you answered yes, please attach any copies with your tender application. *If yes, please provide copies or a link to your plans with your response to this document.*	
	Is a copy of your business continuity plan stored at the backup site and updated regularly?	
	Has a "worst case" scenario to recover normal operations within a prescribed timeframe been implemented and tested?	
	Is your backup site remote from hazards that may endanger the main data centre?	
	Do you include responsibilities for Disaster Recovery Planning in all of your service provider contracts?	
	Are automatic restart and recovery procedures in place to restore data files in the event of a processing failure?	
Compliance: To be completed for **Level 2 and 3**	Are you fully compliant with the requirements of the General Data Protection Regulations? Has this compliance been internally/externally verified? If yes, please advise by whom.	
	Do you undertake Data Protection Privacy Impact Assessments (DPIAs) prior to purchasing new systems, introducing new handling methods and ways of working with personal data?	
	Do you undertake regular audits in relation to your compliance with Cyber and IT security standards?	
	Do you have an identified individual with responsibility for managing any actions arising from internal/external audits undertaken?	
	Do you undertake regular risk assessments in relation to your compliance with Cyber and IT security standards and ensure appropriate mitigation actions are taken?	

HYWEL DDA UNIVERSITY HEALTH BOARD

Part Three
(To be completed by the Third-Party Supplier)
I confirm that the information provided as part of this document to Hywel Dda University Health Board is accurate and correct as of the completion date given below.
Assessment completed by:
Organisation:
Name: Job Title:
Signature:
Date completed:

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.