

INFORMATION GOVERNANCE SUB-COMMITTEE COMMITTEE UPDATE REPORT

Date of last meeting: 18 September 2024

Quoracy: Not Met

Report by: Anthony Tracey, Digital Director, Chair

KEY DISCUSSION POINTS AND MATTERS TO BE ESCALATED FROM THE DISCUSSION AT THE MEETING:

Alert (may require discussion)

The Information Governance Sub-Committee wish to **alert** members of the Sustainable Resource Committee that:

- **Freedom of Information and Environmental Information Policy**– the Sub-Committee approved the changes to the Freedom of Information and Environmental Information Policy.
- **Third Party Supplier Security Policy**– the Sub-Committee approved the changes.

Clinical Coding Update

The Sub-Committee were notified that the Health Board did not meet the clinical coding target for June 2024. The Health Board has ranked fourth out of the eight Health Boards for June 2024 performance (86%). Only two Health Boards, Powys Teaching Health Board and Velindre University NHS Trust achieved the 95% target for June 2024 activity. Hywel Dda University Health Board (HDdUHB), despite not achieving the target, was still well above the all-Wales average of 70.0%.

Advise (to monitor)

The Information Governance Sub-Committee wish to **advise** members of the Sustainable Resource Committee that:

- **Records Management Code of Practice** – amendments have been made to the All-Wales Code of Practice, included splitting the retention guidance into separate categories: GP/Primary Care, Local Authorities, Secondary Care, Community, Mental Health and Corporate. An additional appendix will be added to cover off any Inquires that may present in the future. Health Boards have already been through past Inquires (Goddard/IBI) and whilst current ongoing Inquires such as Thirlwall and David Fuller are not specifically related to patient records, it is likely there may be a requirement for Health Boards to act in the future. The GP section has also been updated to further emphasise the fact that the 20-year long term condition retention guidance will reside within the primary care record, as these records are retained for the life of the patient.

Assure (to note)

The Information Governance Sub-Committee wish to **assure** members of the Sustainable Resource Committee that:

- **Cyber Security Assurance Group** – The Sub-Committee received and approved the revised terms of reference for the sub-group, noting the minor changes to scope of the group in line with the Network and Information Systems (NIS) directive.
- **Corporate and Medical Records Storage Assurance Report** – The Sub-Committee received an update report on the storage of the Swine Flu Vaccination Records and agreed that the files would be brought into the Health Board storage and a retention period allocated to the files.

Review of Risks

The Sub-Committee reviewed the two risks which are aligned to Group. As part of its review, the Sub-Committee considered the status of each risk, and the current score was deemed in tolerance. However, the Sub-Committee did recognise the work that had been done by the Information Governance and Health Records Teams in reducing the risk of inappropriate storage facilities.

Sharing of Learning

The Information Governance Sub-Committee have no matters to alert the Committee on this occasion.

Recommendation

The Committee is asked to:

- **NOTE** the report and **TAKE ASSURANCE** from the actions and oversight of the Sub-Committee
- **REVIEW** and **APPROVE** the following policies:
 - Policy 173 – Freedom of Information and Environmental Information Policy
 - Policy 279 – Third Party Supplier Security Policy
 - Policy 1283 – Misfiling or Mislaid Patient or Staff Records - Reporting and Escalation Procedure

Freedom of Information and Environmental Information Policy

Policy information

Policy number: 173

Classification: Corporate

Supersedes:

Version number: 5

Date of Equality Impact Assessment: 05.08.2024

Approval information

Approved by:

Sustainable Resources Committee

Date of approval:

Date made active:

Review date:

Summary of document:

This policy states our commitment as a Health Board to meet the requirements of the Freedom of Information Act 2000, Environmental Information Regulations 2004 and associated guidance from the Lord Chancellor and the Information Commissioner's Office and outlines mechanisms for ensuring this takes place

Scope:

This policy applies to those members of staff that are employed by the Hywel Dda University Health Board, both permanent and non-permanent, and for whom the Health Board has legal responsibility including contractors and those who undertake work on behalf of contractors

To be read in conjunction with:

[174 - Re-Use Of Public Sector Information Policy](#) (opens in a new tab)

[224 - Information Classification Policy](#) (opens in a new tab)

[201 – All Wales Disciplinary Policy](#) (opens in a new tab)

[249 – Access to Health Records Policy](#) (opens in a new tab)

[836 – AW Information Governance Policy](#) (opens in a new tab)

Patient information:

Include links to [Patient Information Library](#)

Owning group:

IGSC 18.09.2024

Executive Director job title:

Board Secretary

Reviews and updates:

Version 1 – new policy 1.3.2014

Version 2 – reviewed 14.6.2013 Amended flowchart 30.7.2013

Version 3 – reviewed 26.6.2018 link to new AW IG policy added 11.9.2019

Version 4 – complete review 21.12.2021

Version 5 -

Keywords

FOI; Freedom of Information, FOIA, EIR, Environmental Information

Glossary of terms

FOI - Freedom of Information

EIR - Environmental Information Regulations 2004

UK GDPR - UK General Data Protection Regulations

DPA 18 – Data Protection Act 2018

Contents

| | |
|---|----|
| Introduction | 5 |
| Policy Statement..... | 5 |
| Scope | 5 |
| Aim | 6 |
| Definitions | 6 |
| Freedom of Information Act 2000 | 6 |
| Environmental Information Regulations 2004 | 6 |
| Publication Scheme..... | 6 |
| General Rights of Access..... | 7 |
| Freedom of Information Act 2000 | 7 |
| Environmental Information Regulations 2004 | 7 |
| Exemptions and Exceptions..... | 7 |
| Charges and Fees | 8 |
| Freedom of Information 2000 | 8 |
| Environmental Information Regulations 2004..... | 8 |
| Refusal of Requests | 8 |
| Duty to Provide Advice and Assistance | 9 |
| Transferring Requests for Information | 9 |
| Consultation with Third Parties | 9 |
| Managing Contracts | 10 |
| Internal Review process..... | 11 |
| Records Management..... | 11 |
| Training | 11 |
| RESPONSIBILITIES..... | 12 |
| Health Board | 12 |
| Chief Executive | 12 |
| Executive Team | 12 |
| Board Secretary..... | 12 |
| Senior Corporate Information Officer | 12 |
| Freedom of Information Officer | 12 |
| Information Governance Sub-Committee | 13 |
| All staff, Independent Board Members and Contractors..... | 13 |

Line managers..... 13
Implementation 13
Standards and Key Performance Indicators..... 13
Monitoring Compliance..... 13
References..... 14
Appendix A – [OBJ]..... 15
Appendix B – Internal review PROCESS FLOWCHART 16

Introduction

This document sets out the Freedom of Information and Environmental Information Policy for Hywel Dda University Health Board (Health Board). It explains what Hywel Dda University Health Board will do to meet its obligations under the Freedom of Information Act 2000 (hereafter referred to as the Act) and Environmental Information Regulations 2004 (hereafter referred to as the Regulations).

This policy is guided by the *Code of Practice under Section 45 of the Freedom of Information Act 2000* and the *Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004 issued under Regulation 16 of the Regulations*.

This policy is supported by operational procedures for help in complying with both the Act and the Regulations.

The Act replaces the Code of Practice on Openness in the NHS.

Policy Statement

The Health Board supports the Government's commitment to greater openness in the public sector. The Act will further this aim of greater openness, by enabling members of the public to be able to access key information, encouraging an open and transparent view of its activity. The Health Board will make such information available in a range of formats, as required, to meet the needs of the person requesting the information.

The Health Board believes that individuals also have a right to privacy and confidentiality. This policy does not overturn the common law duty of confidence or the statutory provisions that prevent disclosure of personal identifiable information. The release of such information is covered by the General Data Protection Regulations 2016 and Data Protection Act 2018 which replaced the Data Protection Act 1998, and the Access to Health Records Act 1990, and is dealt with in other relevant policies including the Health Board's 238 – Information Governance Framework and 249 - Access to Health Records documents. However, it must be noted that some personal information may be released under the provisions of the Act.

Scope

This policy applies to all Health Board employees, contractors and those who undertake work on behalf of contractors.

Aim

The aim of the policy will be to provide a framework within which the Health Board will operate to ensure its compliance with the statutory legislation.

Definitions

Freedom of Information Act 2000

“The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- Public Authorities are obliged to publish certain information about their activities
- Members of the public are entitled to request information from public authorities

The Act covers any recorded information that is held by a public authority.” ICO, 2021

Environmental Information Regulations 2004

“The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities. The Regulations do this in two ways:

- Public authorities must make environmental information available proactively
- Members of the public are entitled to request environmental information from public authorities.

The Regulations cover any recorded information held by a public authority.” ICO,2021

Publication Scheme

Section 19 of the Act makes it the duty of every public authority to adopt a Publication Scheme.

The Health Board’s Publication Scheme details the information that it has published or intends to publish in the future. It details the format in which the information is available and whether or not a charge will be made for the provision of that information. The Publication Scheme is available on the Health Board’s website <https://hduhb.nhs.wales/about-us/governance-arrangements/freedom-of-information/our-publication-scheme/> (opens in a new tab) and is downloadable free of charge. The contents of the Publication Scheme will be reviewed and updated on an annual basis.

The Health Board publishes the responses to its requests for information under FOI and EIR on its disclosure log, which can be accessed via the following link:

<https://hduhb.nhs.wales/about-us/governance-arrangements/freedom-of-information/disclosure-log/>

(opens in a new tab).

General Rights of Access

Freedom of Information Act 2000

The Act stipulates that requests for information under the General Rights of Access must be received in writing and include the name of the requestor, an address for correspondence and a description of the information requested. As long as the request has a valid address for acknowledgment and response, this is acceptable. The Freedom of Information Officer will be able to provide assistance, if necessary. Requests transmitted by electronic means will be treated as written requests if they are received in legible form and contain sufficient information to process the request.

Under the Act, public authorities may take up to 20 working days to respond.

Environmental Information Regulations 2004

The Regulations state that requests for information can be made either verbally or in writing, although as a response is always required to be in writing, a name and contact details for correspondence will be required.

Under the Act, public authorities may take up to 20 working days to respond.

Exemptions and Exceptions

Under both the Act and the Regulations, the expectation is that the information being requested will be disclosed. However, there are certain conditions whereby information may be withheld and these are subject to an exemption under the Act and an exception under the Regulations. There are two categories of exemptions and exceptions, absolute and qualified.

Absolute – The decision to apply these exemptions/exceptions is final and do not need to be balanced with the public interest test.

Qualified – The decision to apply these exemptions/exceptions must be balanced by the public interest test.

Public Interest Test

The public interest will be considered in every case where a qualified exemption/exception may apply. Defining the public interest will vary according to the information being requested. It may often involve issues around accountability, transparent decision making and good management. When considering the public interest test in order to reach a decision on a qualified exemption/exception, the Health

Board may seek appropriate professional advice (including legal advice) and comments from any third parties such as contractors, external companies etc.

Details of the exemptions/exceptions may be found on the Information Commissioner's Office website at www.ico.org.uk. (opens in a new tab).

The final decision on whether to apply an exemption/exception will be taken by the Freedom of Information Officer.

Charges and Fees

Freedom of Information 2000

The Health Board will operate in accordance with the Freedom of Information (Appropriate Limit and Fees) Regulations 2004. These will determine appropriate limits on charges and fees, how they may be calculated and in what circumstances no fee should be levied. In exceptional circumstances, the Health Board may, at its own discretion, waive any applicable fees.

The following activities may be taken into account when estimating the cost of compliance, which is calculated at £25 per hour up to a limit of £450 (18 hours of staff time):

- determining whether the information is held;
- finding the requested information, or records containing the information;
- retrieving the information or records; and
- extracting the requested information from records.

Environmental Information Regulations 2004

A charge can be levied for any request under the Regulations. However, any charge must be reasonable and take account of the aim of the Regulations, which is to encourage straightforward access to environmental information.

The Health Board will use its discretion on when to apply a charge, and the final decision on this shall be taken by the Freedom of Information Officer.

Refusal of Requests

If the Health Board intends to refuse a request for information, the requestor will be informed of the reasons for this decision within 20 working days. The requestor will also be informed of their rights, conferred by Section 50 of the Act and Regulation 11, to appeal to the Information Commissioner

against the decision, if they are not satisfied with the outcome of the Health Board's internal review procedure.

If the Health Board decides to refuse to confirm or deny whether it holds the information requested and/or to refuse to provide that information, an exemption notice will be issued to the requestor within 20 working days which will:

- State the fact;
- Specify the exemption/exception in question; and
- Explain why the exemption/exception applies.

Duty to Provide Advice and Assistance

The Health Board will ensure that systems and procedures are in place to provide advice and assistance to members of the public who propose to make or have made requests for information. This is a duty under Section 16 of the Act and Regulation 9.

The Health Board will ensure that the systems and procedures to provide advice and assistance also conform to the Code of Practice under Section 45 of the Freedom of Information Act 2000 and the Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004 issued under regulation 16 of the Regulations.

Transferring Requests for Information

When responding to requests for information, The Health Board can only provide information that it holds. If it receives a request for information which it does not hold (or holds only in part) but which is held by another public authority, then it will consider what would be the most helpful way of assisting the requestor with their request. This is likely to involve:

- Informing the requestor that the information requested may be held by another public authority;
- Suggesting that the requestor re-applies to that authority;
- Providing the requestor with contact details for that authority;
- Transferring a request to the other body where they hold information relating to part of a request made to the Health Board, and vice versa, in line with this policy. Any transfer of the request must be with the consent of the requestor.

Consultation with Third Parties

There will be instances where information requested under the Act and the Regulations will include information relating to third parties (i.e. references to organisations or individuals other than the Health Board). Such information will normally be disclosed unless:

- It is "personal data", as defined by the UK GDPR and in guidance issued by the Information Commissioner;

- Where disclosure without consent would constitute an actionable breach of confidence as described in Section 41 of the Act;
- Where a common law duty of confidence is owed (e.g. information concerning a deceased patient).

Where none of the conditions described above apply and where there are no other exemptions, the Health Board will normally be obliged to disclose the information requested. The Health Board will write to third parties to advise them of what information is being released and ask them to notify any concerns. However, the final decision rests with the Health Board.

The Health Board will only accept information from third parties in confidence if it is necessary to obtain that information in connection with the exercise of any of their functions and it would not be otherwise provided.

The Health Board will not agree to hold information received from third parties “in confidence” unless the information has the necessary quality of confidence. Acceptance of any confidentiality provisions must be for good reasons and capable of being justified to the Information Commissioner.

Managing Contracts

When entering into contracts, the Health Board will refuse to include contractual terms which seek to restrict the disclosure of information relating to the contract, beyond the restrictions permitted by the Act and the Regulations. Unless an exemption provided for under the Act or an exception provided under the Regulations is applicable in relation to any particular information, the Health Board will retain the right to disclose that information in response to a request, regardless of the terms of the contract.

When entering into contracts with non-public authority contractors, the Health Board may be asked to accept confidentiality clauses so that information relating to the terms of the contract, its value and performance are exempt from disclosure. Such clauses will be rejected wherever possible. Where exceptionally, it is necessary to include non-disclosure provisions in a contract, the Health Board will investigate the option of agreeing with the contractor a schedule of the contract which clearly identifies information which should not be disclosed. When drawing up any such schedule, the Health Board will be mindful that any restrictions on disclosure could potentially be overridden by obligations under the Act and that such confidentiality provisions must be for good reasons and be capable of being justified to the Information Commissioner’s Office.

In order to avoid unnecessary secrecy, any such constraints on disclosure will be drawn as narrowly as possible and according to the individual circumstances of the case. Apart from such cases, the Health Board will not impose terms of secrecy on contractors.

Internal Review process

The requestor has a right to request the Health Board to undertake an internal review if they are dissatisfied with the response. Internal reviews will be investigated by an Executive Director and the outcome of the review will be formally documented and communicated to the requestor in writing within 20 working days.

When conducting an internal review of an FOI response, the following key factors will be considered:

- Whether the requestor was given adequate advice and guidance about their request for information;
- Whether the procedures for responding to requests for information were followed correctly in this instance;
- Whether, if an exemption/exception was applied, the reasons were explained adequately to the requestor.

Where information has been withheld, the application of any exemption/exception will be re-examined, as will any application of the public interest test in the case of a qualified exemption/exception.

When responding to requests for information, the Freedom of Information Officer will inform the requestor of the procedure for an internal review, as well as advising them of their right of appeal to the Information Commissioner's Office.

If the requestor is still dissatisfied following the internal review process, the individual can appeal further to the Information Commissioner's Office if they feel that the Health Board has not complied with its obligations under the Freedom of Information Act 2000 or Environmental Information Regulations 2004.

Records Management

The Health Board has systems and processes in place for managing its corporate records in both electronic and paper format in order to respond effectively to requests for information.

Training

Freedom of Information and Environmental Information training is available to all staff via the corporate induction programme. The Senior Corporate Information Officer is responsible for arranging any additional specific training for staff groups.

A staff guide to Freedom of Information and Environmental Information requests is available on the intranet or on request from the Freedom of Information team. Additionally, a short guide to FOI and EIR is accessible to the public, via the Health Board's website, as well as being issued as an attachment with all acknowledgements.

RESPONSIBILITIES

Health Board

The Health Board needs to have secure and robust information governance processes in place to ensure it meets its statutory responsibilities. Information Governance encompasses all aspects of information handling including Freedom of Information and Environmental Information.

Chief Executive

The Chief Executive has ultimate responsibility for the organisation's compliance with the Act and the Regulations. Responsibility for bringing FOI/EIR issues to the Board is delegated to the Board Secretary.

Executive Team

The Executive Team is responsible for managing the internal review process, with a named Executive Director allocated to investigate internal reviews.

Board Secretary

The Board Secretary has overall responsibility for the corporate function of the Health Board, including FOI and EIR requests.

Senior Corporate Information Officer

The Senior Corporate Information Officer will provide support and guidance to the Freedom of Information Officer, to ensure that the Health Board remains compliant with its duties under the Act and Regulations.

The Senior Corporate Information Officer will also ensure that all processes and procedures put in place have been tested to ensure they meet the requirements of the Act and the Regulations.

Freedom of Information Officer

The Freedom of Information Officer will manage the day to day FOI/EIR function, and ensure that all requests are fulfilled in accordance with the Health Board's statutory duty.

Information Governance Sub-Committee

The Information Governance Sub-Committee reports to the Sustainable Resource Committee and comprises of key staff from the Health Board. The Information Governance Sub-Committee will oversee the development and updating of this policy and related procedures and ensure that awareness of FOI/EIR is maintained across the Health Board.

All staff, Independent Board Members and Contractors

All staff, Independent Board members, contractors and those who undertake work on behalf of contractors are obliged to adhere to this policy. They should be familiar with the requirements of the Act and the Regulations and be aware of their personal responsibilities under the legislation.

Line managers

Line managers must ensure that their staff are aware of this policy and how to deal with Freedom of Information and Environmental Information requests should they receive one.

Implementation

It will be the responsibility of the Senior Corporate Information Officer to ensure that this policy is implemented effectively across the Health Board, through training.

Information Governance issues, including Freedom of Information and Environmental Information, will be highlighted on a routine basis through the Information Governance Sub-Committee to the Sustainable Resource Committee.

Standards and Key Performance Indicators

The Senior Corporate Information Officer will regularly assess performance in meeting the standards and statutory timeframes of the *Code of Practice under Section 45 of the Freedom of Information Act 2000* and the *Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004* issued under regulation 16 of the Regulations.

Monitoring Compliance

The Health Board will review the Freedom of Information and Environmental Information arrangements to ensure compliance with this policy.

The FOI Officer will maintain records of all FOI/EIR requests for monitoring purposes in accordance with the Codes of Practice.

The Senior Corporate Information Officer will produce quarterly reports to the Information Governance Sub-Committee under delegated authority from Strategic Development and Operational Delivery Committee, to assess performance in meeting the statutory timeframes.

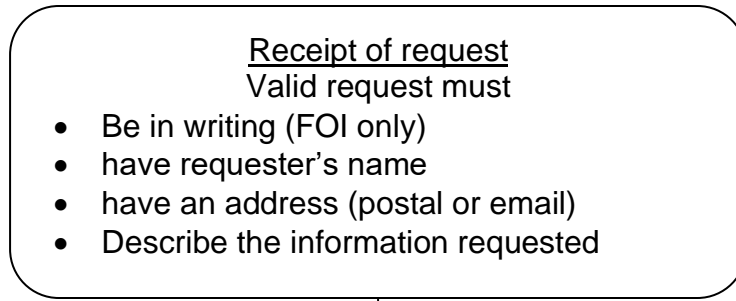
References

- Freedom of Information Act 2000 – <http://www.legislation.gov.uk/ukpga/2000/36/contents>
- Information Commissioners Office Freedom of Information Act webpage - http://www.ico.gov.uk/what_we_cover/freedom_of_information.aspx
- Code of Practice under Section 45 of the Freedom of Information Act 2000 - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/744071/CoP_FOI_Code_of_Practice_-_Minor_Amendments_20180926_.pdf
- Environmental Information Regulations 2004 - <https://www.legislation.gov.uk/uksi/2004/3391/made>
- Information Commissioners Office Environmental Information Regulations webpage – <http://ico.org.uk/for-organisations/guide-to-the-environmental-information-regulations/>
- Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004 issued under regulation 16 of the Regulations – <https://ico.org.uk/media/for-organisations/documents/2013835/eir-regulation-16-code-of-practice.pdf>

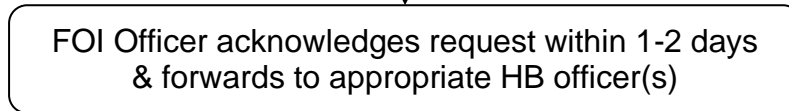
Appendix A – [OBJ]

DAY 1

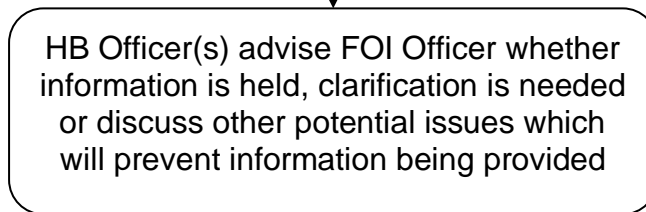
Day 1 is the first day it arrives in the organisation not in the FOI Office



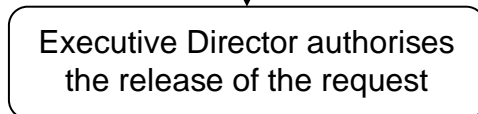
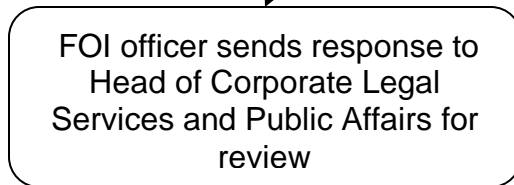
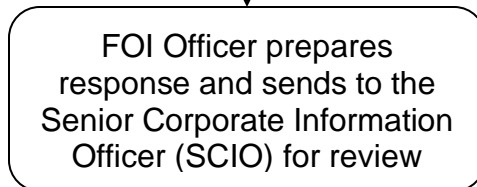
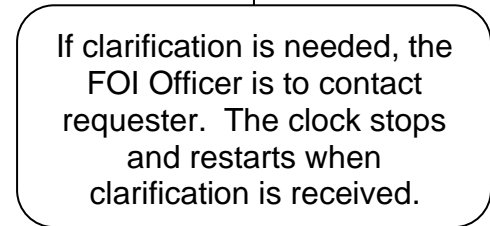
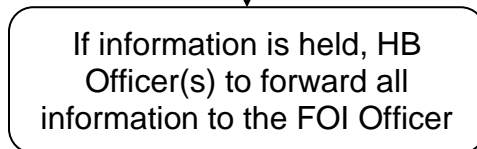
BY DAY 2



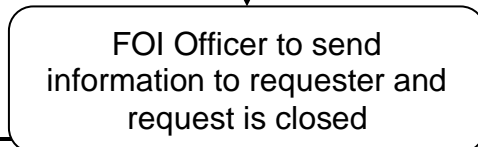
BY DAY 4



BY DAY 10



BY DAY 20



Appendix B – Internal review PROCESS FLOWCHART

DAY 1

Day 1 is the first day it arrives in the organisation not in the FOI Office

Receipt of internal review

- Requestor dissatisfied with Health Board response, appeal to Health Board received.
- Must be in writing (FOI only)
- Must include requester's name
- Must include an address (postal or email)
- Must contain the reasons for appealing the response

BY DAY 2

FOI Officer acknowledges internal review within 1-2 days and forwards to named Executive Director

BY DAY 10

Board Secretary conducts a review to establish:

- The procedures for responding to the request were followed correctly.
- All information, relevant to the request, held by the Health Board, was provided to the requestor.
- Where any information was withheld, the application of exemption/s used was done so correctly and explained fully.

BY DAY 20

Following completion of the review, the named Executive Director drafts the appeal response and sends to the requestor

Equality Impact Assessment (EqIA) Screening Template

When to complete an EqIA Screening

An EqIA Screening Template must be completed when reviewing, changing and developing procedures/ proposals/ projects/ policies. This is a first step and is used to consider whether there are any negative impacts that may arise.

Purpose of an EqIA Screening Template

The purpose of this short exercise is to ensure that you have shown appropriate due regard when considering the impact for people with protected characteristics in your decision making. The screening process is designed to help you consider the circumstances and to inform evidence-based decisions.

If the proposal is of a significant nature and it is apparent from the outset that a full EqIA will be required, then it is not necessary to complete this Screening Template, you can proceed to complete the full [EqIA](#).

If no negative impacts are identified following completion of the EqIA screening then it is not necessary to undertake a full EqIA however, the decision and justification must be clearly recorded in this document.

On completion of the Screening Template:

- Ensure that all the white boxes within the screening are completed.
- Ensure that the Procedure/ Project/ Proposal/ Policy owner has signed and dated the Screening Template.
- Send a copy of the completed template along with the related policy or project proposal to Inclusion.hdd@wales.nhs.uk for the Diversity & Inclusion Team to review.
- Each Screening Template will be reviewed by the Diversity & Inclusion Team and feedback will be provided to the Procedure/ Project/ Proposal/ Policy owner. This may include recommendations for further action to inform robust decision-making.

Support

For further support please visit the [EqIA Sharepoint](#) or contact:

Email: Inclusion.hdd@wales.nhs.uk

Tel: 01554 899055

| | |
|---------------------------------|-------------------------------------|
| Director and Directorate | Joanne Wilson, Corporate Governance |
| Service Area | Corporate Office |

| | |
|--|--|
| Title of Procedure, Project, Proposal, Policy being screened: | 173 - Freedom of Information and Environmental Information Policy |
|--|--|

Description of the Procedure/ Project/ Proposal/ Policy being screened (including key aims and objectives)

This policy states our commitment as a Health Board to meet the requirements of the Freedom of Information Act (the Act) and Environmental Information Regulations (the Regulations) and associated guidance from the Lord Chancellor and the Information Commissioner's office and outlines mechanisms for ensuring this takes place.

The aim of the policy will be to provide a framework within which the Health Board will ensure compliance with the requirements of the Act and the Regulations and will underpin any operational procedures and activities connected with the implementation of the Act and the Regulations.

The aim of this policy will be met by ensuring that a process is in place which is followed by all relevant Health Board staff.

Evidence considered (including staff and population data, relevant research, expert and community knowledge etc.)

The Freedom of Information Act (FOIA) 2000 and Environmental Information Regulations 2004, are part of the Government's commitment to greater openness in the public sector. The Act and Regulations further this aim by helping to transform the culture of the public sector to one of greater openness. It will enable members of the public and other groups to question the decisions of public authorities more closely, ensuring that the services the Health Board provides are effectively and properly delivered.

References

- Freedom of Information Act 2000 – <http://www.legislation.gov.uk/ukpga/2000/36/contents>
- Information Commissioners Office Freedom of Information Act webpage - [http://www.ico.gov.uk/what we cover/freedom of information.aspx](http://www.ico.gov.uk/what_we_cover/freedom_of_information.aspx)
- Code of Practice under Section 45 of the Freedom of Information Act 2000 - [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/744071/CoP FOI Code of Practice - Minor Amendments 20180926 .pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/744071/CoP_FOI_Code_of_Practice_-_Minor_Amendments_20180926_.pdf)
- [Environmental Information Regulations 2004 - https://www.legislation.gov.uk/uksi/2004/3391/made](https://www.legislation.gov.uk/uksi/2004/3391/made)
- [Information Commissioners Office Environmental Information Regulations webpage – http://ico.org.uk/for-organisations/guide-to-the-environmental-information-regulations/](http://ico.org.uk/for-organisations/guide-to-the-environmental-information-regulations/)

- Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004 issued under regulation 16 of the Regulations –

<https://ico.org.uk/media/for-organisations/documents/2013835/eir-regulation-16-code-of-practice.pdf>

Assess which protected characteristics will potentially be affected by the proposal in the table below (please ✓ the relevant box to confirm positive, negative or no impact).

If at any point a negative impact has been identified (actual or potential), you do not need to proceed with the completion of this form, as a full EqlA must be undertaken: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](#)

| | | | | |
|---|--------------------------|-----------------|--------------------------|---|
| Age | | | | |
| Is it likely to affect older and younger people in different ways or affect one age group and not another? | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact <input checked="" type="checkbox"/> |
| Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis. | | | | |
| Disability | | | | |
| Is it likely to affect those with a physical disability, learning disability, sensory loss or impairment, mental health conditions, long-term medical conditions such as diabetes? | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact <input checked="" type="checkbox"/> |
| Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis. | | | | |
| Gender Reassignment | | | | |
| Is it likely to affect those who either: | | | | |
| <ul style="list-style-type: none"> • Have undergone, intend to undergo or are currently undergoing gender reassignment. • Do not intend to undergo medical treatment but wish to live in a different gender from their gender at birth | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact <input checked="" type="checkbox"/> |
| Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis. | | | | |
| Marriage / Civil Partnership | | | | |
| Under the Equality Act, the characteristic of Marriage and Civil Partnerships is only protected in the workplace/ employment. Is it likely to affect those who are married or in a Civil Partnership? This means someone who is legally married or in a civil partnership. | | | | |

| | | | | | |
|--|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| <p>Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.</p> | | | | | |
| <p>Pregnancy and Maternity Is it likely to affect those who are pregnant or have recently had a baby? Maternity covers the period of 26 weeks after having a baby, whether or not they are on Maternity Leave.</p> | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| <p>Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.</p> | | | | | |
| <p>Race / Ethnicity Is it likely to affect people of a different race, nationality, colour, culture or ethnic origin including non-English / Welsh speakers, Gypsies/Travellers, asylum seekers and migrant workers?</p> | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| <p>Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.</p> | | | | | |
| <p>Religion or Belief Is it likely to affect people who have a religion or belief? The term 'religion' includes a religious or philosophical belief.</p> | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| <p>Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.</p> | | | | | |
| <p>Sex Is it likely to affect people who are mostly male or female. Where it applies to both equally does it affect one differently to the other?</p> | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| <p>Justification of impact identified: After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.</p> | | | | | |

Sexual Orientation

Whether a person's sexual attraction is towards their own sex, the opposite sex or either.

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified:
 After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.

Armed Forces Community

Consider whether this impacts on members of the Armed Forces and their families, whose health needs may be impacted long after they have left the Armed Forces and returned to civilian life. Also consider their unique experiences when accessing and using day-to-day public and private services compared to the general population. It could be through 'unfamiliarity with civilian life, or frequent moves around the country and the subsequent difficulties in maintaining support networks, for example, members of the Armed Forces can find accessing such goods and services challenging.'

For a comprehensive guide to the Armed Forces Covenant Duty and supporting resource please see:

[Armed-Forces-Covenant-duty-statutory-guidance](#)

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified:
 After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.

Socio Economic Duty

Consider those on low income, economically inactive, unemployed or unable to work due to ill-health. Also consider people living in areas known to exhibit poor economic and/or health indicators and individuals who are unable to access services and facilities. Food / fuel poverty and personal or household debt should also be considered.

For a comprehensive guide to the Socio-Economic Duty in Wales and supporting resources please see:

[more-equal-wales-socio-economic-duty](#)

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified:
 After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no impact of the policy in relation to human rights. The FOI Act details a set of rules which deem a request to be valid, all requests that are compliant with these stipulations are processed in accordance with the Act on an applicant and purpose blind basis.

Welsh Language

Is it likely to impact on opportunities for people to use the Welsh language? The Welsh language should be treated no less favourably than the English language.

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified:
 After a full review of the document to ensure the document was accessible and easily understandable, there is still a low relevance to the equality duties and no

impact of the policy in relation to human rights. All requests are treated equitably whether received in Welsh or English, responses are translated into the Welsh language before issuing.

If a negative impact has been identified, you are not required to complete this form as a full EqlA must be undertaken. A full EqlA template and guidance can be found on the following link: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](#)

| | | |
|--|-----------------|--|
| Screening Completed by: | Name | Katie Jenner |
| | Title | Senior Corporate Information Officer |
| | Contact details | Katie.jenner@wales.nhs.uk |
| | Date | 24.07.2024 |
| Screening Authorised by: (Directorate level owner of the procedures/ proposals/ projects/ policy) | Name | Katie Jenner |
| | Title | Senior Corporate Information Officer |
| | Contact details | Katie.jenner@wales.nhs.uk |
| | Date | 24.07.2024 |
| Guidance has been provided by Diversity & Inclusion Team: | Name | Alan Winter |
| | Title | Senior Diversity & Inclusion Officer |
| | Contact details | Alan.winter@wales.nhs.uk |
| | Date | 5/8/2024 |
| Diversity and Inclusion Team additional Comments: | | |

Please note: The D&I team will save a copy of the completed form for reference. If any changes are made after the date of review, it is the directorate's responsibility to update the EqlA and inform the D&I team.



Third Party Supplier Security Policy

Policy information

Policy number: 279

Classification: Corporate

Supersedes: All previous policies

Version number: 3

Date of Equality Impact Assessment:

[Detail date of EqIA](#)

Approval information

Approved by: Sustainable Resources Committee

Date of approval:

Date made active:

Review date:

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'

HYWEL DDA UNIVERSITY HEALTH BOARD

- 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

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.

HYWEL DDA UNIVERSITY HEALTH BOARD

Contents

| | |
|--|----|
| Introduction..... | 4 |
| Policy Statement | 4 |
| Scope | 4 |
| Aim | 5 |
| Objectives..... | 5 |
| Process to be followed | 5 |
| Before commencing the tender process or entering into any agreement with a third-party supplier. | 5 |
| Overview of main tasks to be completed..... | 5 |
| Task 1: Completing the Third-Party Supplier Screening Document | 6 |
| No personal/sensitive information shared (Level 0 access to information) | 6 |
| Low level access to information (Level 1 access to information)..... | 6 |
| Moderate level/risk access to information (Level 2 access to information) | 7 |
| High level/risk access to information (Level 3 access to information) | 7 |
| NB: If the individual responsible is not going through procurement for the purposes of the contract or agreement they must follow below steps themselves..... | 8 |
| Roles and Responsibilities..... | 10 |
| References | 11 |
| Appendix 1a – complete the third party supplier screening and third party supplier security questionnaires..... | 12 |
| Appendix 1b – task 2 carry out a data protection impact assessment if required | 13 |
| Appendix 1c – task three: checking contract/agreement arrangements | 14 |
| Appendix 2 Third party supplier screening document..... | 15 |
| Appendix 3 - Third Party Supplier Security Questionnaire | 19 |
| Appendix 4 - Key terms to be included in any contract for level 1 and above information sharing/access with a third party supplier | 34 |

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 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

HYWEL DDA UNIVERSITY HEALTH BOARD

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.

HYWEL DDA UNIVERSITY HEALTH BOARD

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.

HYWEL DDA UNIVERSITY HEALTH BOARD

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

HYWEL DDA UNIVERSITY HEALTH BOARD

intrusive e.g. cold calling at their home phone number or address, sending sensitive information to a home address that could be seen 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

HYWEL DDA UNIVERSITY HEALTH BOARD

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.

HYWEL DDA UNIVERSITY HEALTH BOARD

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

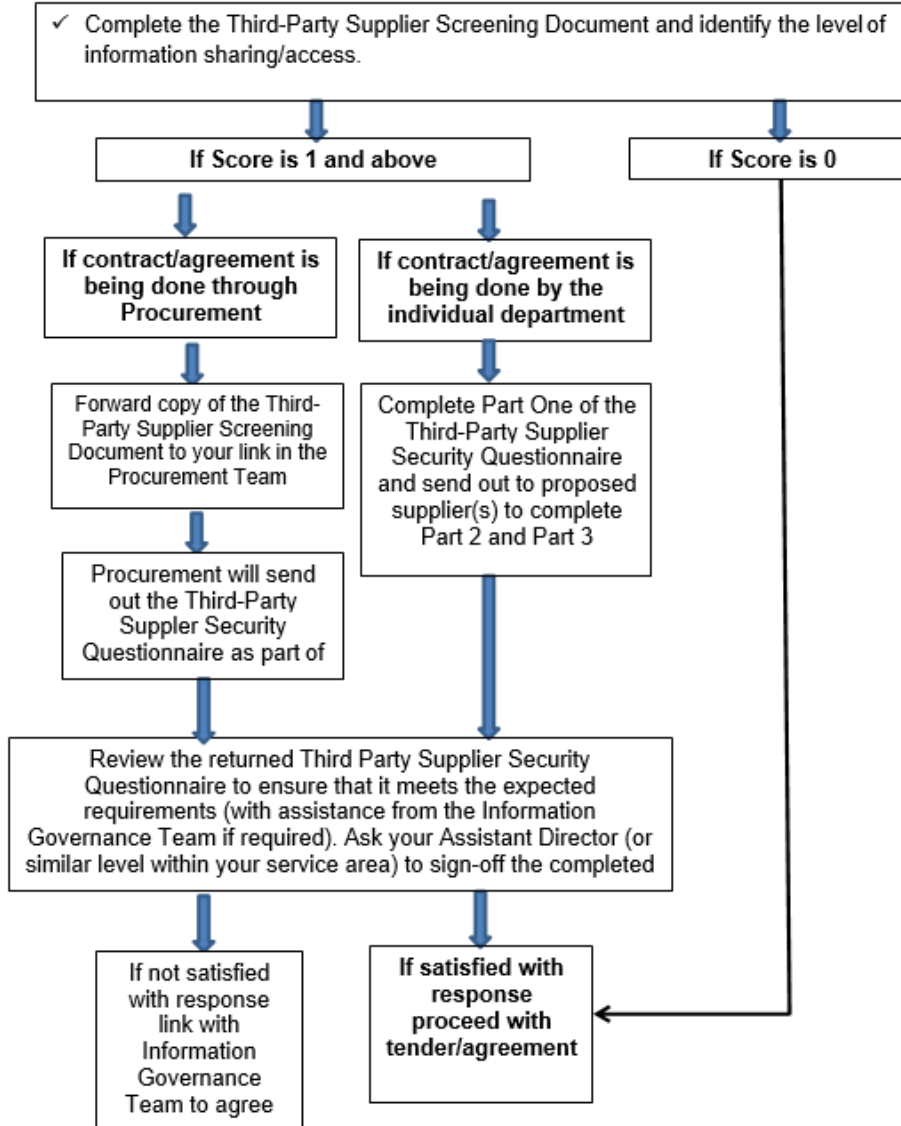
Caldicott Guardian at: CaldicottGuardian.HDD@wales.nhs.uk

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

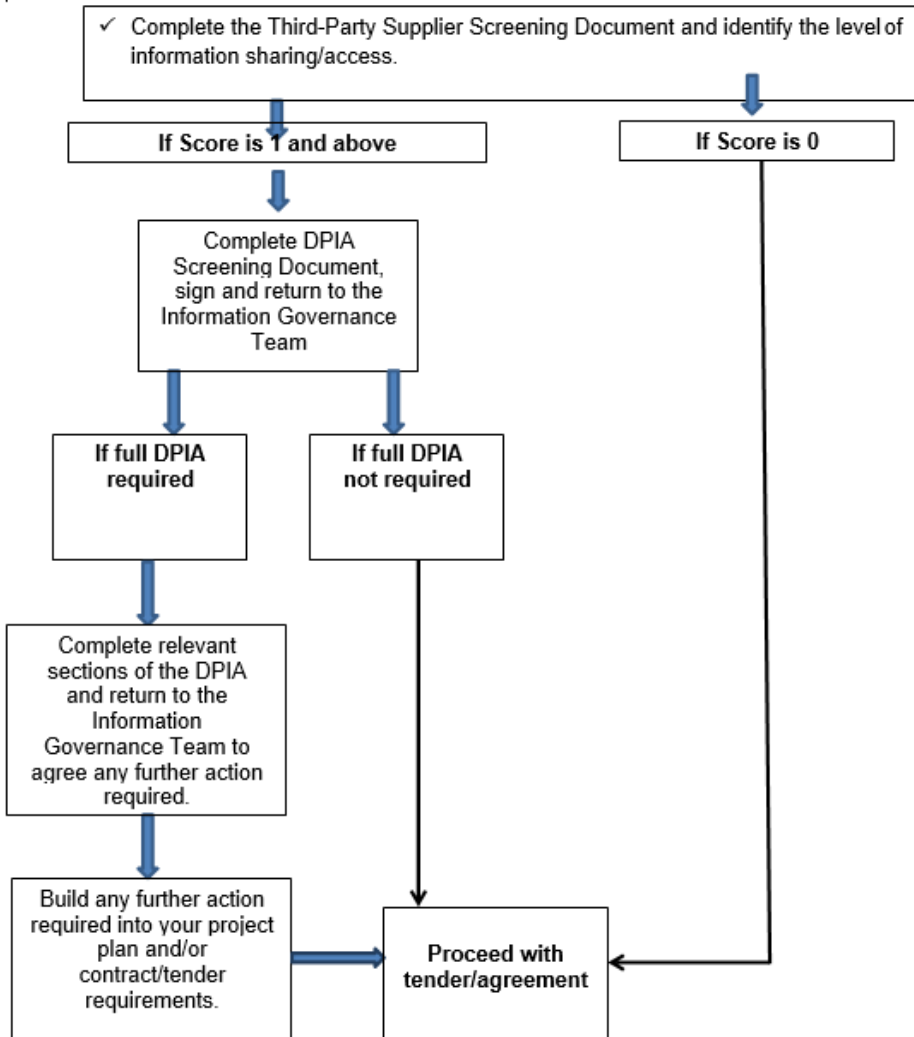
11. Appendix 1a – Task One: Complete the Third-Party Supplier Screening and Third-Party Supplier Security Questionnaires.



HYWEL DDA UNIVERSITY HEALTH BOARD

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

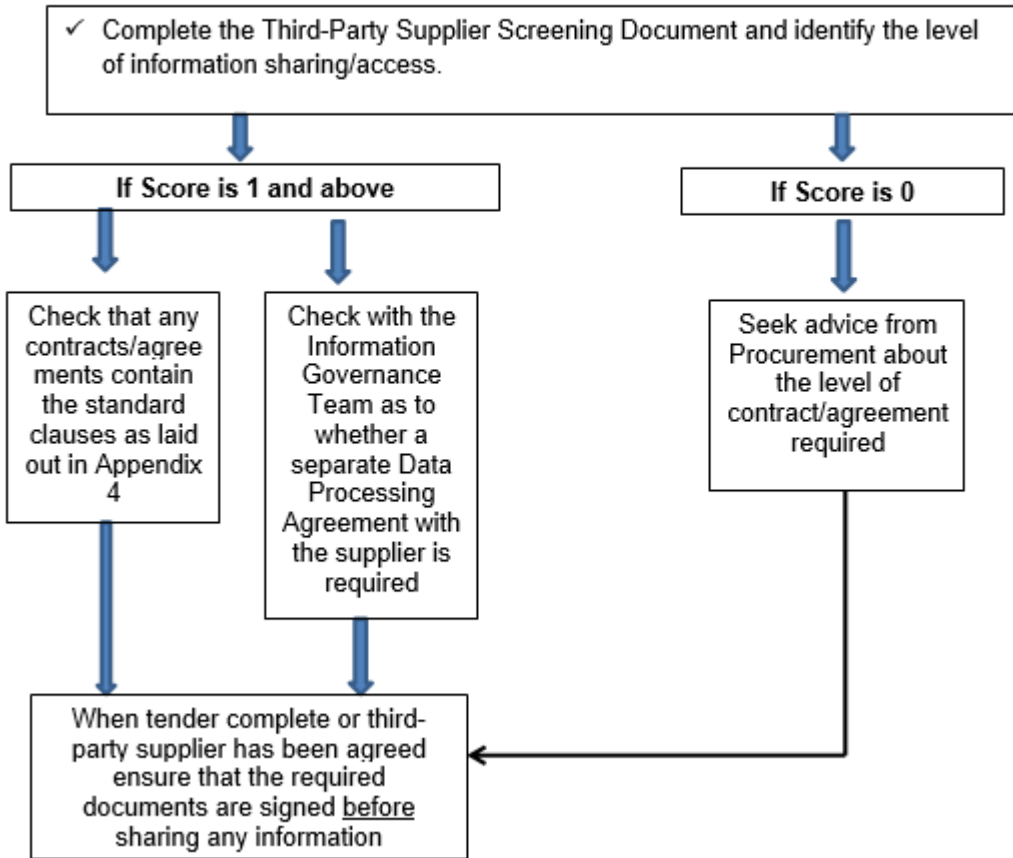
Checklist for staff before entering into a third-party supplier agreement or contract
12. Appendix 1b – Task Two: Carry out a Data Protection Impact Assessment (DPIA) if required



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: <ul style="list-style-type: none">• 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. <p>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).</p> | Level 0 |

HYWEL DDA UNIVERSITY HEALTH BOARD

| | |
|--|----------------|
| Low level/risk access to information | Level 1 |
| <ul style="list-style-type: none"> • 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. <p>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.</p> | |
| Moderate level/risk access to information | Level 2 |
| <ul style="list-style-type: none"> • 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 <u>within UK</u>. • 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 <u>will not</u> be removed by the supplier from a Health Board site. <p>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.</p> | |

HYWEL DDA UNIVERSITY HEALTH BOARD

| High level/risk access to information | Level 3 |
|---|---------|
| <ul style="list-style-type: none"> • 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. <p>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.</p> | |

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 | | <ol style="list-style-type: none"> 1. No further action required. 2. Proceed with your tender process as normal. |

HYWEL DDA UNIVERSITY HEALTH BOARD

| | | |
|-------|--|--|
| 1 - 3 | | <p>Before commencing the tender process</p> <ol style="list-style-type: none">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. <p>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 it is returned and completed before entering into any formal agreement.</p> <p>Before entering into a contract or formal agreement</p> <ol style="list-style-type: none">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

Appendix 3 - Third Party Supplier Security Questionnaire



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? <i>If yes, please provide copies or a link to your policies with your response to this document.</i> | |
| | 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? <i>If yes, please provide copies or a link to your policies with your response to this document.</i> | |
| 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 | |

Part Two

279

25 of 32

Version2

HYWEL DDA UNIVERSITY HEALTH BOARD

| | | |
|--|---|--|
| | 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 policies, 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? | |

HYWEL DDA UNIVERSITY HEALTH BOARD

| | | |
|---|--|--|
| 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 | |

HYWEL DDA UNIVERSITY HEALTH BOARD

| | | |
|---|--|--|
| | 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 data 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'? <i>If yes, please advise where the information will be stored.</i> | |

HYWEL DDA UNIVERSITY HEALTH BOARD

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).

HYWEL DDA UNIVERSITY HEALTH BOARD

| | | |
|---|---|--|
| 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? <i>ISO 27001</i> <i>Cyber Essentials</i> | |
| To be completed for Level 3 | Do you hold certification against the following that has been verified by an appropriate certification body? <i>Cyber Essentials Plus</i> <i>If yes, please provide evidence of your certification when returning this form</i> | |
| 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? | |

HYWEL DDA UNIVERSITY HEALTH BOARD

| | | |
|--|---|--|
| 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 | |
|--|---|--|

HYWEL DDA UNIVERSITY HEALTH BOARD

| | | |
|--|---|--|
| for Level 2 and 3 | <p>this agreement? If you answered yes, please attach any copies with your tender application.</p> <p><i>If yes, please provide copies or a link to your plans with your response to this document.</i></p> | |
| | 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.

HYWEL DDA UNIVERSITY HEALTH BOARD

- 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.

Equality Impact Assessment (EqIA) Screening Template

When to complete an EqIA Screening

An EqIA Screening Template must be completed when reviewing, changing and developing procedures/ proposals/ projects/ policies. This is a first step and is used to consider whether there are any negative impacts that may arise.

Purpose of an EqIA Screening Template

The purpose of this short exercise is to ensure that you have shown appropriate due regard when considering the impact for people with protected characteristics in your decision making. The screening process is designed to help you consider the circumstances and to inform evidence-based decisions.

If the proposal is of a significant nature and it is apparent from the outset that a full EqIA will be required, then it is not necessary to complete this Screening Template, you can proceed to complete the full [EqIA](#).

If no negative impacts are identified following completion of the EqIA screening then it is not necessary to undertake a full EqIA however, the decision and justification must be clearly recorded in this document.

On completion of the Screening Template:

- Ensure that all the white boxes within the screening are completed.
- Ensure that the Procedure/ Project/ Proposal/ Policy owner has signed and dated the Screening Template.
- Send a copy of the completed template along with the related policy or project proposal to Inclusion.hdd@wales.nhs.uk for the Diversity & Inclusion Team to review.
- Each Screening Template will be reviewed by the Diversity & Inclusion Team and feedback will be provided to the Procedure/ Project/ Proposal/ Policy owner. This may include recommendations for further action to inform robust decision-making.

Support

For further support please visit the [EqIA Sharepoint](#) or contact:

Email: Inclusion.hdd@wales.nhs.uk

Tel: 01554 899055

| | |
|---------------------------------|------------------------|
| Director and Directorate | Digital Services |
| Service Area | Information Governance |

| | |
|--|--------------------------------------|
| Title of Procedure, Project, Proposal, Policy being screened: | Third Party Supplier Security Policy |
|--|--------------------------------------|

Description of the Procedure/ Project/ Proposal/ Policy being screened (including key aims and objectives)

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.

This policy will ensure that the Health Board complies with its statutory duties laid out in the UK General Data Protection Regulation 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.

Evidence considered (including staff and population data, relevant research, expert and community knowledge etc.)

We have considered the staff that this procedure applies to.

Assess which protected characteristics will potentially be affected by the proposal in the table below (please ✓ the relevant box to confirm positive, negative or no impact).

If at any point a negative impact has been identified (actual or potential), you do not need to proceed with the completion of this form, as a full EqlA must be undertaken: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](https://sharepoint.com)

| | | | | |
|--|--------------------------|-----------------|--------------------------|-------------------------------------|
| Age | | | | |
| Is it likely to affect older and younger people in different ways or affect one age group and not another? | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact |
| | | | | <input checked="" type="checkbox"/> |
| Justification of impact identified: This policy has the same impact on a person regardless of their age, therefore no impact identified. | | | | |
| Disability | | | | |

| | | | | | |
|--|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Is it likely to affect those with a physical disability, learning disability, sensory loss or impairment, mental health conditions, long-term medical conditions such as diabetes? | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| Justification of impact identified: This policy has the same impact on a person regardless of their disability, therefore no impact identified. | | | | | |
| Gender Reassignment | | | | | |
| Is it likely to affect those who either: | | | | | |
| <ul style="list-style-type: none"> • Have undergone, intend to undergo or are currently undergoing gender reassignment. • Do not intend to undergo medical treatment but wish to live in a different gender from their gender at birth | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| Justification of impact identified: This policy has the same impact on a person regardless of their gender, therefore no impact identified. | | | | | |
| Marriage / Civil Partnership | | | | | |
| Under the Equality Act, the characteristic of Marriage and Civil Partnerships is only protected in the workplace/ employment. | | | | | |
| Is it likely to affect those who are married or in a Civil Partnership? This means someone who is legally married or in a civil partnership. | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| Justification of impact identified: This policy has the same impact on a person regardless of their marital status, therefore no impact identified. | | | | | |
| Pregnancy and Maternity | | | | | |
| Is it likely to affect those who are pregnant or have recently had a baby? Maternity covers the period of 26 weeks after having a baby, whether or not they are on Maternity Leave. | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| Justification of impact identified: This policy has the same impact on a person regardless of their Health, therefore no impact identified. | | | | | |
| Race / Ethnicity | | | | | |
| Is it likely to affect people of a different race, nationality, colour, culture or ethnic origin including non-English / Welsh speakers, Gypsies/Travellers, asylum seekers and migrant workers? | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| Justification of impact identified: This policy has the same impact on a person regardless of their race, therefore no impact identified. | | | | | |
| Religion or Belief | | | | | |
| Is it likely to affect people who have a religion or belief? The term 'religion' includes a religious or philosophical belief. | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
| Justification of impact identified: This policy has the same impact on a person regardless of their religion or beliefs, therefore no impact identified. | | | | | |
| Sex | | | | | |
| Is it likely to affect people who are mostly male or female. Where it applies to both equally does it affect one differently to the other? | | | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |

Justification of impact identified: This policy has the same impact on a person regardless of their sex therefore no impact identified.

Sexual Orientation

Whether a person's sexual attraction is towards their own sex, the opposite sex or either.

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified: This policy has the same impact on a person regardless of their sexual choices, therefore no impact identified.

Armed Forces Community

Consider whether this impacts on members of the Armed Forces and their families, whose health needs may be impacted long after they have left the Armed Forces and returned to civilian life. Also consider their unique experiences when accessing and using day-to-day public and private services compared to the general population. It could be through 'unfamiliarity with civilian life, or frequent moves around the country and the subsequent difficulties in maintaining support networks, for example, members of the Armed Forces can find accessing such goods and services challenging.'

For a comprehensive guide to the Armed Forces Covenant Duty and supporting resource please see:

[Armed-Forces-Covenant-duty-statutory-guidance](#)

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified: This policy has the same impact on a person regardless of their previous job roles, therefore no impact identified.

Socio Economic Duty

Consider those on low income, economically inactive, unemployed or unable to work due to ill-health. Also consider people living in areas known to exhibit poor economic and/or health indicators and individuals who are unable to access services and facilities. Food / fuel poverty and personal or household debt should also be considered.

For a comprehensive guide to the Socio-Economic Duty in Wales and supporting resources please see:

[more-equal-wales-socio-economic-duty](#)

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified: This policy has the same impact on a person regardless of their income or where they live, therefore no impact identified.

Welsh Language

Is it likely to impact on opportunities for people to use the Welsh language? The Welsh language should be treated no less favourably than the English language.

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | <input checked="" type="checkbox"/> |
|-----------------|--------------------------|-----------------|--------------------------|-----------|-------------------------------------|

Justification of impact identified: This policy has the same impact on a person regardless of their language, therefore no impact identified.

If a negative impact has been identified, you are not required to complete this form as a full EqlA must be undertaken. A full EqlA template and guidance can be found on the following link: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](#)

| | | |
|--|-----------------|---------------------------------|
| Screening Completed by: | Name | Sarah Bevan |
| | Title | Information Governance Manager |
| | Contact details | Sarah.Bevan3@wales.nhs.uk |
| | Date | 09/10/2024 |
| Screening Authorised by: (Directorate level owner of the procedures/ proposals/ projects/ policy) | Name | Patrycja Duszynska |
| | Title | Head of Information Governance |
| | Contact details | patrycja.duszynska@wales.nhs.uk |
| | Date | 09/10/2024 |
| Guidance has been provided by Diversity & Inclusion Team: | Name | |
| | Title | |
| | Contact details | |
| | Date | |
| Diversity and Inclusion Team additional Comments: | | |

Please note: The D&I team will save a copy of the completed form for reference. If any changes are made after the date of review, it is the directorate's responsibility to update the EqIA and inform the D&I team.

MISFILING OR MISLAID PATIENT OR STAFF RECORDS - REPORTING AND ESCALATION PROCEDURE

Procedure information

Procedure number: 1283

Classification: Corporate

Supersedes: N/A

Version number: 1

Date of Equality Impact Assessment: 05/08/2024

Approval information

Approved by: Sustainable resources Committee

Date of approval:

Date made active:

Review date:

Summary of document:

This document includes the correct procedure to be used by staff when information has been misfiled or mislaid within the Hywel Dda University Health Board.

Scope:

Persistent unavailability of care records leads to gaps in clinical knowledge and also means that the Health Board becomes vulnerable to not being able to respond to patients who wish to see records that are held about them.

Staff records must be treated with the same level of protection as patient records.

To be read in conjunction with:

[320 – Acceptable Use of IT Policy](#) – opens in a new tab

[172 – Confidentiality 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

[201 - All Wales Disciplinary Policy and Procedure](#) – opens in a new tab

[435 - All Wales NHS Staff to Raise Concerns Procedure \(Whistleblowing\)](#) – opens in a new tab

[1088 - Information Rights Procedure](#) – opens in a new tab

Patient information:

Include links to [Patient Information Library](#)

Owning group:

Information Governance Sub Committee

Date signed off by owning group

Executive Director job title: Director of Finance

Reviews and updates:

1.0 New Procedure

Keywords

Audit, WPAS, Medical Records, Patient Records, Information Governance, Staff files

Glossary of terms

| | |
|--------------------------------------|---|
| Caldicott Guardian | A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. |
| Data Protection Legislation | Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and transparent about why personal data is being collected, and how the data is going to be used, stored and shared. |
| Personal Data | Personal Data is information which relates to a living individual who can be identified from the information itself or by linking it with other information – for example a person's name and address, an online profile, a member of staff's HR record or records relating to individual's such as patients or service users. |
| Personal Data Breach | A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. |
| Senior Information Risk Owner (SIRO) | An Executive Director or member of the Senior Management Board with overall responsibility for information risk across the Health Board. |
| Special Category Data | Special category data means personal data consisting of information as to: <ul style="list-style-type: none">- Genetic and biometric data- Political opinions- Religious or other beliefs- Trade union membership- Physical or mental health/condition- Sexual life And although not specifically described as special category data, this information requires the same treatment: <ul style="list-style-type: none">- The commission or alleged commission of any offence- Any proceedings for any offence committed/alleged to have been committed, the disposal of such proceedings or the sentence of such proceedings |

Contents

| | |
|---|----|
| Scope | 4 |
| Aim | 4 |
| Objectives | 4 |
| INTRODUCTION | 4 |
| PROCEDURE | 4 |
| Reporting & Investigating a missing patient or staff record. | 5 |
| When missing Records are found. | 7 |
| Misfiling within Records | 8 |
| TRAINING | 9 |
| IMPLEMENTATION | 9 |
| REVIEW | 9 |
| REFERENCES | 9 |
| APPENDIX 1 – LOGGING A MISSING RECORD ON DATIX | 10 |

Scope

All staff with access to electronic clinical systems will be affected by the introduction of this procedure. The Health Board needs to be able to evidence that it knows where all of its records reside and, where it does not, that it has a process in place to ensure their effective retrieval. The Health Board also needs to ensure that if misfiling occurs, this is documented, investigated and staff are supported so they feel confident they can fulfil their job roles effectively.

Aim

The aim of this document is to:

- Ensure the availability of records required for all patient care.
- Ensure that any records that cannot be found are reported and investigated.
- Comply with the Data Protection Act 2018 and UK GDPR.
- Educate staff that lack of availability of information is a potential personal data breach.

Objectives

The aim of this document will be achieved by the following objectives:

- Identify and DATIX all incidents of misfiling found on paper and electronic records.
- Identify and DATIX all mislaid files.
- Escalate any potential Personal Data Breaches to the Information Governance team so that action can be taken.
- Where a case has to be answered, inform the Workforce Department to follow the processes outlined within this procedure and which may result in action being taken in line with the Health Board's [Disciplinary Policy and Procedure](#) (opens in a new tab).

INTRODUCTION

Persistent unavailability of care records leads to gaps in clinical knowledge and also means that the Health Board becomes vulnerable to not being able to respond to patients who wish to see records that are held about them. Staff records must be treated with the same level of protection as patient records.

The Health Board needs to be able to evidence that it knows where all of its records reside and, where it does not, that it has a process in place to ensure their effective retrieval. This procedure enables the Health Board to demonstrate its commitment to complying with the Data Protection Act 2018 and UK GDPR.

PROCEDURE

The Procedures follow several steps to identify and escalate potential personal data breaches:

Reporting & Investigating a missing patient or staff record.

In the event of health or staff records being lost or stolen from Health Board premises and/or other locations. The following table shows the step-by-step process that can be followed by staff:

| Step | Who | Task |
|------|---|--|
| 1 | Staff Member | Identifies that a paper patient/staff record is missing, or a file contains incorrect information: <ul style="list-style-type: none"> • Was transit from one location to another – not arrived • Within the Acute Hospitals or Health Board offices • At medical records storage |
| 2 | Staff Member | Inform Line Manager of missing record, or misfiled information. |
| 3 | Staff Member and/or Team Colleagues | Missing records <ul style="list-style-type: none"> • Carry out a thorough search of all areas occupied and used by the team including all desk drawers, cupboards and storage areas that would not routinely be used for storing records. • For files missing in transit, contact both the intended recipient and sender to check that the record has not been delivered but is misplaced at its destination or within the mail system. Contact any other Health Board sites along its transportation route for searches to be undertaken in case it has been incorrectly delivered elsewhere. • This search must not delay the incident being reported on DATIX. |
| 4 | Staff Member or Line Manager | Report the missing record or misfiling immediately (and in any event within 24 hours) via DATIX incident reporting system: <ul style="list-style-type: none"> • The name of the staff member reporting the incident. • Patient ID. NHS number may also be recorded in the additional details section. • A brief description of the file's last known movements. • A physical description of the file (e.g. green wallet). • Any other file barcode number associated with that record. |
| 5 | Health Records & Information Governance Teams | For files missing in transit, request confirmation of how it was sent: <ul style="list-style-type: none"> • Exactly how it was addressed. • What service was used - Internal vs external post. • Date of sending (with electronic patient records this should be logged on WPAS tracking). • Was an acknowledgement form used and returned to sender. • Was a return address used. • If external mail was used, then identify the tracking number. • The route the post usually takes from sender to recipient – try to identify if it has been mis-delivered. • Has a warning pop up been added to WPAS to say the notes are missing? • Review electronic audit trail in case any other use may have accessed the record. • Re-check all areas for the missing file. |

| | | |
|---|--|---|
| | | |
| 6 | Health Records & Information Governance Teams | Check the audit trail for the electronic files to see if the file tracking is being used correctly. Contact all staff concerned if files are not being tagged correctly. |
| 7 | Health Records Teams / Service Area (e.g. Therapies / Workforce) | <p>If lost externally (storage company), retrieve boxes sent for archiving at the same time as the missing file and check for misfiling.</p> <p>If lost internally (Health Board medical records storage), check boxes in vicinity of record, check file locations with similar references. If you are able to identify the date the file was returned check what other files were returned on that date.</p> |
| 8 | Health Records Teams | If the record has been missing for 6 months it is reasonable to assume that the original records are not going to become available unless found by chance. Create a duplicate set of records from the temporary set and print the word REPLACEMENT in large, black capital letters on the front of the folder. These can be merged if the original record is found. |

When missing Records are found.

When a member of staff identifies or finds a missing record, they must take responsibility to follow this procedure. The following table shows the step-by-step process that can be followed by staff:

| Step | Who | Task |
|------|--|---|
| 1 | Staff Member | Inform Line Manager. |
| 2 | Staff Member / Line Manager / Health Records | Update the DATIX. |
| 3 | Staff Member / Line Manager / | Notify Health I Records or Workforce. |
| 4 | Staff Member / Line Manager / Health Records | Make arrangements for the original and replacement records to be merged, disposing of any duplicated documents in the confidential waste. |
| 5 | Staff Member / Line Manager / Health Records | Inform Information Governance that the record has been found. |

Misfiling within Records

When a member of staff identifies a record contains incorrect information or information about another person, they must take responsibility to follow this procedure. The following table shows the step-by-step process that can be followed by staff:

| Step | Who | Task |
|------|---|---|
| 1 | Staff Member | Inform Line Manager. |
| 2 | Staff Member / Line Manager / Health Records / Workforce | Identify all the misfiled information within the record and Log the incident on DATIX. |
| 3 | Staff Member / Line Manager / | Notify Health Records or Workforce that incorrect information has been found within a record. |
| 4 | Staff Member / Line Manager / Health Records / Workforce | Make arrangements for the original record to be rectified e.g. informing IT that a digital record needs to be amended (CarePartner / WPAS / WCP etc). Make arrangements to remove misfiling from an incorrect paper record, and identify the record that the information belongs to. You may need support from Health Records or Information Governance with this. Make sure you dispose of any duplicated documents in the confidential waste. |
| 5 | Staff Member / Line Manager / Health Records | Update DATIX and Inform Information Governance that the record has been rectified and is now correct. |
| 6 | Information Governance team | If the member of staff who misfiled the information can be identified, invite them to attend IG training. |

TRAINING

All staff will be required to have appropriate Information Governance training, additional training can be requested by individuals or line managers. Training will be provided in several formats to accommodate all learning styles and the requirements of staff and The Health Board.

IMPLEMENTATION

Communication exercises have been undertaken to ensure all staff groups are aware of this procedure and the implications of any breaches identified. This will be further supported through Information Governance communications via Globals / Newsletters / IG Awareness on Intranet.

REVIEW

This Procedure will be reviewed in line with the further roll out and enforcement of the policy rules, or sooner, as required.

REFERENCES

Information Commissioner Office <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

APPENDIX 1 – LOGGING A MISSING RECORD ON DATIX

Guidance for logging the incident on Datix – missing files

| Incident Type | |
|------------------|---------------------------|
| * Classification | Records, Information |
| * Category | Healthcare record |
| * Sub Category | Missing healthcare record |

| Additional Information | |
|--|-----|
| * Was any equipment involved in the incident? | |
| * Did medication have a direct impact on this incident? | |
| * Does this Incident have Information Governance considerations? <small>The answer should be 'yes' if the incident involves personal or sensitive data, including near misses. For example, a breach of confidentiality, theft, loss or misuse of personal data, information security, etc. For further advice, please contact your information governance team</small> | Yes |

Misfiling

| Incident Type | |
|------------------|---|
| * Classification | Records, Information |
| * Category | Healthcare record |
| * Sub Category | Documents misfiled in healthcare record (wrong patient) |

| Additional Information | |
|--|-----|
| * Was any equipment involved in the incident? | |
| * Did medication have a direct impact on this incident? | |
| * Does this Incident have Information Governance considerations? <small>The answer should be 'yes' if the incident involves personal or sensitive data, including near misses. For example, a breach of confidentiality, theft, loss or misuse of personal data, information security, etc. For further advice, please contact your information governance team</small> | Yes |

Equality Impact Assessment (EqIA) Screening Template

When to complete an EqIA Screening

An EqIA Screening Template must be completed when reviewing, changing and developing procedures/ proposals/ projects/ policies. This is a first step and is used to consider whether there are any negative impacts that may arise.

Purpose of an EqIA Screening Template

The purpose of this short exercise is to ensure that you have shown appropriate due regard when considering the impact for people with protected characteristics in your decision making. The screening process is designed to help you consider the circumstances and to inform evidence-based decisions.

If the proposal is of a significant nature and it is apparent from the outset that a full EqIA will be required, then it is not necessary to complete this Screening Template, you can proceed to complete the full [EqIA](#).

If no negative impacts are identified following completion of the EqIA screening then it is not necessary to undertake a full EqIA however, the decision and justification must be clearly recorded in this document.

On completion of the Screening Template:

- Ensure that all the white boxes within the screening are completed.
- Ensure that the Procedure/ Project/ Proposal/ Policy owner has signed and dated the Screening Template.
- Send a copy of the completed template along with the related policy or project proposal to Inclusion.hdd@wales.nhs.uk for the Diversity & Inclusion Team to review.
- Each Screening Template will be reviewed by the Diversity & Inclusion Team and feedback will be provided to the Procedure/ Project/ Proposal/ Policy owner. This may include recommendations for further action to inform robust decision-making.

Support

For further support please visit the [EqIA Sharepoint](#) or contact:

Email: Inclusion.hdd@wales.nhs.uk

Tel: 01554 899055

| | |
|---------------------------------|------------------------|
| Director and Directorate | Digital Services |
| Service Area | Information Governance |

| | |
|--|--|
| Title of Procedure, Project, Proposal, Policy being screened: | Misfiling or mislaid patient or staff records - reporting and escalation procedure |
|--|--|

Description of the Procedure/ Project/ Proposal/ Policy being screened (including key aims and objectives)

This procedure is to be used by staff when information has been misfiled or mislaid within the Hywel Dda University Health Board. The Health Board needs to be able to evidence that it knows where all of its records reside and, where it does not, that it has a process in place to ensure their effective retrieval. The Health Board also needs to ensure that if misfiling occurs, this is documented, investigated and staff are supported so they feel confident they can fulfil their job roles effectively. The aim of this document is to, ensure the availability of records required for all patient care, ensure that any records that cannot be found are reported and investigated, ensure compliance with the Data Protection Act 2018 and UK GDPR, and to educate staff that lack of availability of information is a potential personal data breach.

Evidence considered (including staff and population data, relevant research, expert and community knowledge etc.)

We have considered the staff that this procedure applies to.

Assess which protected characteristics will potentially be affected by the proposal in the table below (please ✓ the relevant box to confirm positive, negative or no impact).

If at any point a negative impact has been identified (actual or potential), you do not need to proceed with the completion of this form, as a full EqlA must be undertaken: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](https://sharepoint.com)

| | | | |
|--|--------------------------|-----------------|---|
| Age | | | |
| Is it likely to affect older and younger people in different ways or affect one age group and not another? | | | |
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input checked="" type="checkbox"/> No Impact |
| Justification of impact identified: This policy has the same impact on a person regardless of their age, therefore no impact identified. | | | |
| Disability | | | |
| Is it likely to affect those with a physical disability, learning disability, sensory loss or impairment, mental health conditions, long-term medical conditions such as diabetes? | | | |

| | | | | | |
|--|--|-----------------|--|-----------|---|
| Positive Impact | | Negative Impact | | No Impact | x |
| Justification of impact identified: This policy has the same impact on a person regardless of their disability, therefore no impact identified. | | | | | |
| Gender Reassignment | | | | | |
| Is it likely to affect those who either: | | | | | |
| <ul style="list-style-type: none"> • Have undergone, intend to undergo or are currently undergoing gender reassignment. • Do not intend to undergo medical treatment but wish to live in a different gender from their gender at birth | | | | | |
| Positive Impact | | Negative Impact | | No Impact | x |
| Justification of impact identified: This policy has the same impact on a person regardless of their gender, therefore no impact identified. | | | | | |
| Marriage / Civil Partnership | | | | | |
| Under the Equality Act, the characteristic of Marriage and Civil Partnerships is only protected in the workplace/ employment. | | | | | |
| Is it likely to affect those who are married or in a Civil Partnership? This means someone who is legally married or in a civil partnership. | | | | | |
| Positive Impact | | Negative Impact | | No Impact | x |
| Justification of impact identified: This policy has the same impact on a person regardless of their marital status, therefore no impact identified. | | | | | |
| Pregnancy and Maternity | | | | | |
| Is it likely to affect those who are pregnant or have recently had a baby? Maternity covers the period of 26 weeks after having a baby, whether or not they are on Maternity Leave. | | | | | |
| Positive Impact | | Negative Impact | | No Impact | x |
| Justification of impact identified: This policy has the same impact on a person regardless of their Health, therefore no impact identified. | | | | | |
| Race / Ethnicity | | | | | |
| Is it likely to affect people of a different race, nationality, colour, culture or ethnic origin including non-English / Welsh speakers, Gypsies/Travellers, asylum seekers and migrant workers? | | | | | |
| Positive Impact | | Negative Impact | | No Impact | x |
| Justification of impact identified: This policy has the same impact on a person regardless of their race, therefore no impact identified. | | | | | |
| Religion or Belief | | | | | |
| Is it likely to affect people who have a religion or belief? The term 'religion' includes a religious or philosophical belief. | | | | | |
| Positive Impact | | Negative Impact | | No Impact | x |
| Justification of impact identified: This policy has the same impact on a person regardless of their religion or beliefs, therefore no impact identified. | | | | | |
| Sex | | | | | |
| Is it likely to affect people who are mostly male or female. Where it applies to both equally does it affect one differently to the other? | | | | | |
| Positive Impact | | Negative Impact | | No Impact | x |

Justification of impact identified: This policy has the same impact on a person regardless of their sex therefore no impact identified.

Sexual Orientation

Whether a person's sexual attraction is towards their own sex, the opposite sex or either.

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | x |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|

Justification of impact identified: This policy has the same impact on a person regardless of their sexual choices, therefore no impact identified.

Armed Forces Community

Consider whether this impacts on members of the Armed Forces and their families, whose health needs may be impacted long after they have left the Armed Forces and returned to civilian life. Also consider their unique experiences when accessing and using day-to-day public and private services compared to the general population. It could be through 'unfamiliarity with civilian life, or frequent moves around the country and the subsequent difficulties in maintaining support networks, for example, members of the Armed Forces can find accessing such goods and services challenging.'

For a comprehensive guide to the Armed Forces Covenant Duty and supporting resource please see:

[Armed-Forces-Covenant-duty-statutory-guidance](#)

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | x |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|

Justification of impact identified: This policy has the same impact on a person regardless of their previous job roles, therefore no impact identified.

Socio Economic Duty

Consider those on low income, economically inactive, unemployed or unable to work due to ill-health. Also consider people living in areas known to exhibit poor economic and/or health indicators and individuals who are unable to access services and facilities. Food / fuel poverty and personal or household debt should also be considered.

For a comprehensive guide to the Socio-Economic Duty in Wales and supporting resources please see:

[more-equal-wales-socio-economic-duty](#)

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | x |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|

Justification of impact identified: This policy has the same impact on a person regardless of their income or where they live, therefore no impact identified.

Welsh Language

Is it likely to impact on opportunities for people to use the Welsh language? The Welsh language should be treated no less favourably than the English language.

| | | | | | |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|
| Positive Impact | <input type="checkbox"/> | Negative Impact | <input type="checkbox"/> | No Impact | x |
|-----------------|--------------------------|-----------------|--------------------------|-----------|---|

Justification of impact identified: This policy has the same impact on a person regardless of their language, therefore no impact identified.

If a negative impact has been identified, you are not required to complete this form as a full EqlA must be undertaken. A full EqlA template and guidance can be found on the following link: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](#)

| | | |
|--|-----------------|--|
| Screening Completed by: | Name | Sarah Bevan |
| | Title | Information Governance Manager |
| | Contact details | Sarah.Bevan3@wales.nhs.uk |
| | Date | 24/07/2024 |
| Screening Authorised by: (Directorate level owner of the procedures/ proposals/ projects/ policy) | Name | Patrycja Duszynska |
| | Title | Head of Information Governance |
| | Contact details | patrycja.duszynska@wales.nhs.uk |
| | Date | 24/07/2024 |
| Guidance has been provided by Diversity & Inclusion Team: | Name | Kylie Daniels |
| | Title | Senior Diversity and Inclusion Officer |
| | Contact details | Kylie.daniels@wales.nhs.uk |
| | Date | 05/08/2024 |
| Diversity and Inclusion Team additional Comments: | | |

Please note: The D&I team will save a copy of the completed form for reference. If any changes are made after the date of review, it is the directorate's responsibility to update the EqIA and inform the D&I team.