IG07 Final V9

PROCEDURE FOR DEALING WITH SUBJECT ACCESS REQUESTS UNDER DATA PROTECTION LEGISLATION

Author & Title	[redacted]						
Responsible dept / director:	[redacted]						
Approved by:	[redacted]						
Date approved:	19/08/2021						
Date activated (live):	January 2012						
Documents to be read alongside this document:	All Wales Information Governance Policy Your Information Your Rights (YIYR) Leaflet IG01 Records Management Policy IG02 Records Management Procedure IG04 Access to Information Policy HR4 Access to Health Records Procedure All Wales Email Policy IG08 Email Procedure IG13 Confidentiality Code of Conduct IG14 Procedure for Information Management and Technology (IM&T) Security IG15 Procedure for Storage and Transportation of Personal Data or Sensitive Information IG16 Procedure for Staff on Disclosing Personal Data IG24 Notification of Information Security Breach Procedure WP6 BCUHB Code of Conduct (Disciplinary Rules and Standards of Behaviour)						
Date of next review:	July 2024						
First operational:	January 2012						
Previously reviewed:	October 2012	January 2015	March 2017	April 2018	August 2021		
Changes made yes/no:	Yes	Yes	Yes	Yes	Yes		

N.B. Staff should be discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.

Contents:

1. Introduction

1.1 The Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) are the main pieces of legislation governing the protection of personal data in the UK. Under the legislation any living individual (or their nominated representative i.e. a solicitor or Assembly Member) has the right to contact an organisation and ask to 'view' and / or request a copy of any personal information that the organisation is holding about them. This is known as a Subject Access Request (SAR).

1.2 This procedure details the standard process that should be followed within Betsi Cadwaladr University Health Board (BCUHB) to ensure a consistent approach when dealing with requests for personal information. It supports BCUHB's 'Access to Information Policy' and should be read in conjunction with that policy. It should be noted that this procedure is specifically for requests for personal information not contained within the health record.

1.3 This procedure also details processes to be followed when dealing with requests for information from third parties e.g. Police, solicitors etc.

1.4 The legislation covers all forms and formats of personal information i.e. written, computerised, images, audio / video recordings etc., however if access is required to a health record, a request should be made separately under BCUHB's 'Access to Health Records Procedure (HR4)'.

2. Procedure Statement

GDPR was introduced on 25th May 2018 alongside the DPA 2018, in order to enhance the rights of an individual concerning access to, and copies of, their personal data.

This procedure outlines BCUHB's assurance in respect of managing responses to subject access requests received from the public and third parties across paper and digital, local and national platforms, in accordance with legislation.

3. Aims/Purpose

In accordance with legislation, the procedure will assist BCUHB with:

- processing all Subject Access Requests (SARs) within the legislative timeframe;
- releasing appropriate information in accordance with the legislation;
- providing advice and assistance where appropriate;
- dealing with complaints about any aspect of BCUHB's compliance with the legislation promptly and impartially;
- respecting the interests of third parties who may be affected by any potential disclosure of information.

4. Objectives

This procedure has been developed with the aim of:

- providing guidance for BCUHB staff;
- ensuring continued and improved compliance with legislation;
- supporting and embedding a culture of compliance towards good record keeping standards for all staff who create and handle personal data;
- providing assurance against legislative compliance standards through robust Key Performance Indicators (KPI) and performance management

5. Scope

This procedure applies to all staff employed by or contracted to BCUHB, and includes experts who BCUHB might call upon in consultation.

6. Roles and Responsibilities

6.1 Chief Executive

The Chief Executive has overall responsibility for Data Protection and Confidentiality within BCUHB. As accountable officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support the handling of subject access requests.

6.2 Senior Information Risk Officer

The Director of Finance is also the identified Senior Information Risk Owner (SIRO), and will take ownership of information risk. The SIRO is a key factor in successfully raising the profile of information risks and embedding information risk management into the Health Board's culture.

6.3 Caldicott Guardian

The Caldicott Guardian has specific responsibilities regarding confidentiality and consent, in relation to personal data.

6.4 Data Protection Officer

The Data Protection Officer has delegated responsibilities from the Chief Executive, specifically with regards to compliance with Data Protection legislation and the rights of data subjects.

6.5 All Staff

All staff, whether clinical or administrative, including temporary and agency, have a responsibility to adhere to information governance policies, procedures and standards. Breaches of this document must be reported via the Datix

incident reporting system, and processed in accordance with WP9 Disciplinary Policy where appropriate. This also applies to contractors, students, volunteers and anyone else providing a service on behalf of the Health Board, as well as Health Board employees working from a non-Health Board site.

7. Making a Subject Access Request (SAR)

7.1 Under Data Protection legislation, individuals have the right to access any information an organisation holds about them whether in an electronic or manual format

7.2 Individuals also have the right to:

- know whether their personal information is being processed (which includes being held or stored);
- be given a description of the data held, the purposes for which it is processed, and to whom the data may be disclosed. This includes being told who, within the organisation, has accessed their records;
- be given a copy of the information held;
- be given information as to the source of the data

7.3 Applicants who make contact either in person or by telephone can be provided with a Subject Access Request Form for completion, in order to assist with the processing of the request and to enable a timely and full response. The completed form must be forwarded immediately to the Information Governance team.

Requests may also be received by letter or e-mail and must be directed immediately to a member of the Information Governance team.

7.4 If an applicant objects to completing the form, then a request can be accepted verbally at the point of contact. However, the staff member receiving the request should transcribe, gather as much information as possible, and forward to the Information Governance team.

7.5 Requests from staff members

If a request is received from a member of staff who wishes to access their personal file, in the first instance they should be offered the opportunity to view their personal file on an informal basis. This should be arranged by their line manager and must take place in a quiet area with both parties present.

Should copies of information contained within their personal file be requested, then copies should be supplied as soon as is practically possible. However, if they request a full copy of their file then the SAR process should be followed and the line manager must provide a full photocopy of the original file to the Information Governance Manager (IGM). The original personal file must not be sent to Information Governance.

When a request for a personal file is made, the line manager is responsible for providing a full photocopy of the original file to the Information Governance (IG) Manager. The original personal file is not to be sent to the Information Governance offices.

7.6 Requests from representatives

Individuals with capacity have a right of access to their own personal data. However, an individual can also authorise a third party such as a nominated formal representative, family member or solicitor to do so on their behalf.

The personal representative, usually the Executor or Administrator of the estate, is the only person who has an unqualified right of access to the personal data of the individual concerned. If there is more than one personal representative, consent from all must be provided. Written proof of the relationship will be required i.e. copy of the will / proof of probate.

A person other than the personal representative, who has personally or financially been affected by the terms of the will, may put forward a request in order to make a claim against the estate. This would only apply to a spouse, child, or beneficiary who had been named in the descendants previous will. Written proof of this would have to be provided.

Unless there is a consent form signed during the person's life time, which gives instruction on what to release, statutory obligations only grant that the minimum and relevant information should be released.

7.7 Requests for children's records

Those with parental responsibility may have a statutory right to apply for access to their child's personal data, unless the child is capable of consenting, or there is a safeguarding concern. Prior to disclosure, a professional should give careful consideration to the duty of confidentiality owed to the child. Also whether there are any safeguarding concerns i.e. there is a child protection order or the child has been fostered or adopted.

Children between the ages of 13 and 16 who have the capacity and understanding to make decisions about themselves are also entitled to decide whether their personal information may be disclosed. However, good practice dictates that the child should be encouraged to involve their parents or other legal guardians in such decisions.

Consideration must be given by professionals as to whether they consider the child to have sufficient maturity and understanding to object to the disclosure of their personal data.

7.8 Requests for deceased information

Data Protection / GDPR only applies to information which relates to living individuals. Information relating to a deceased person does not constitute

personal data under the legislation and is therefore not subject to Subject Access Rights.

Any requests for deceased health information can be obtained from the Access to Health Records department, further information can be found in HR4 – Access to Health Records Procedure.

Any requests for deceased non-health information should be processed under FOI, however exemptions to disclosure may apply.

8. Proving right of access

8.1 The applicant will be expected to supply a form of identification, and proof of address as part of their request. These should include at least one copy of either a passport, birth certificate or driving licence, together with either a copy of a utility bill confirming the applicant's current address, or a driving licence (if not already used as proof of identity).

8.2 Requests submitted by a nominated representative (e.g. family member, Solicitor, Assembly Member) acting on behalf of an individual should obtain the individual's consent in writing, and include a copy of this with their request. The consent form must have been signed by the individual within 6 months of the date of request.

8.3 Under Data Protection legislation there is no requirement for an individual to provide a reason for requesting access to their personal data, or what part of the record is required. However, it is considered good practice to contact the applicant to gain clarification of what information is required before processing the request, if it is not clear what is required. This may decrease the time it takes to respond to the applicant and avoid unnecessary delays.

8.4 If a request is submitted in relation to receiving all emails held about them personally, then clarification should be sought on which BCUHB staff members are involved, and a timeframe for the searches. Email searches are conducted by Informatics staff, however they are unable to search all BCUHB Outlook mailboxes at once, due to the volume of mailboxes.

8.5 BCUHB is legally obliged to comply with all SARs within 28 calendar days of receipt of request, however the clock stops until proof of identity is verified.

8.6 A copy of the information requested must be provided free of charge. However, when a request is manifestly unfounded or excessive, particularly if it is repetitive, a 'reasonable fee' can be charged. Please refer to Section 9 below.

9. Processing complex, manifestly unfounded and/or excessive requests

9.1 If in receipt of a SAR which is complex or requires the processing of a large amount of information, the timescale for responding can be extended for up to

two months. The applicant must be notified within one month of receiving the request to explain why the extension is necessary.

9.2 There will normally be no charges for SARs, however, a reasonable fee for administrative costs may be charged if a request is manifestly unfounded or excessive, for example if it is continually repeated and the information has not changed. In this case, the applicant should be notified promptly and BCUHB does not need to comply with the request until the fee has been received.

9.3 A reasonable fee can be charged to comply with requests for further copies of the same information. However, this does not mean a charge can be applied to subsequent SARs.

10. Procedure for processing SARs

10.1 Stage one – receipt of request

10.1.1 SARs may be received at any BCUHB site. If received in writing, the request should be forwarded immediately to the Information Governance team, as the deadline is calculated from the date of receipt into the organisation, not the date received by the Information Governance team. The most efficient way of doing this is to scan and email the request to BCU.DPO@wales.nhs.uk.

10.1.2 On receipt of a SAR the IGA will log the request onto the Datix system, giving each request a unique identifier reference using the following format: <Ascending number>/<year>/SAR i.e. 001/19/SAR

10.1.3 If the applicant has not supplied sufficient information for the request to be processed the IGA will send a standard letter / email with an accompanying SAR form to the applicant, requesting proof of identity. The 'Subject Access and Data Protection legislation' information leaflet should also be sent to assist the individual with their application. The 28 calendar day deadline starts from receipt of the form and proof of identity.

10.2 Stage two – processing the request

10.2.1 On receipt of proof of identify the IGA will verify to ensure that the applicant is authorised to access the information.

10.2.2. Providing there is sufficient information to process the request, the IGA will send the applicant a letter / email of acknowledgement.

10.2.3 If the request is from a nominated representative of the individual, a letter of consent must be included with the request or the SAR form must be completed and appropriately signed.

10.2.4 If there are any doubts as to the legitimacy of consent e.g. date on consent form not within 6 months of date request received, or the amount of information requested, the applicant must be contacted for further clarification.

10.3 Stage three - Collating information

10.3.1 A request for the information required should be sent to the relevant department / manager, and a copy of this request stored as an attachment on Datix. If an individual has requested all information held on them within the organisation, a search of all relevant databases, electronic systems, filing systems (including archived systems) should be initiated.

10.3.2 Due to the complexity and size of BCUHB, some requests may be considered complex in nature. Should this be the case the following steps can be put in place to assist with the retrieval of information to ensure compliance with the timescale:

- The IGM / Senior IG Officer (SIGO) will establish who is involved with the information request (for example W&OD or Medical Workforce, which Clinical or Corporate Division), and contact them to establish where the information may be held.

- The IGM must highlight to the Head of Information Governance (HoIG) immediately where there is concern that the retrieval of information may become complex in nature.

- If no response is received from identified leads within 5 working days, then the IGM must highlight this to HoIG.

- The HoIG will email all identified leads and notify the appropriate Executives / Directors / Assistant Directors (clinical and non-clinical) on the complexity of the case and the need to convene a multi-disciplinary team (MDT) meeting.

- The IGM / SIGO will arrange an MDT with all identified leads (appropriate representation from Departments, W&OD, Head of IG) within 3 working days to discuss concerns and issues raised with the retrieval of the information.

- The MDT will action the retrieval and copying of the information by appropriate leads (who may or may not be present at the meeting) and timescales must set.

- The copied information must be forwarded to the IGM within the next 8 working days.

10.4 <u>Stage three – reviewing the information</u>

10.4.1 All information that has been collated must be carefully reviewed by the IGM / SIGO.

10.4.2 If any ‘third party’ individual is named or has provided information about the applicant, the following must be considered for redaction. Redaction simply means removing information prior to release, and should ideally be undertaken electronically using approved software, which is currently **Nitro**

Pro. Any other methods of redaction used must be carefully checked prior to release to ensure that the information cannot be seen or made visible under any circumstances:

- Is it possible to comply with the request without revealing information which relates to and identifies any third party individuals? If so, the third party information must either be removed prior to disclosure, or alternatively consent of the individuals must be obtained.

- Following discussion with the relevant departmental manager, prior to disclosure, careful consideration must be given to ensure that the applicant would not suffer any harm or distress on receipt of the information.

- If a third party individual does not consent to disclosure, and the IG team are not satisfied that it would be reasonable to disclose the information, it should be withheld.

- However, as much of the information requested should be given without disclosing the identity of the third party where possible unless it is reasonable, given all of the circumstances, to disclose without consent, as ultimately the final decision to disclose lies with BCUHB.

10.4.3 If the third party information has previously been provided to, or is already known by the applicant, or it is generally available, it would be considered reasonable to disclose the information without third party consent.

10.4.4 Datix must be updated with details of the course of action and reasoning behind why consent was not sought, or considered not appropriate.

10.4.5 Information must be checked thoroughly to ensure that any codes or acronyms are explained to the applicant.

10.4.6 It must be decided by the IGM / SIGO whether there are any grounds for exempting the information under the legislation. Examples include safeguarding, national security and crime and taxation. If the exemption to withhold relates to safeguarding, then the clinician responsible for that area of care should provide the rationale for withholding, which should be recorded against the record of request. The applicant does not have to be provided with this rationale but the clinician should be aware that they may have to present it in court if necessary.

10.4.7 Any police requests included within the personal information should not be routinely disclosed without considering the following:

- How long is it since the police request was received i.e. is the investigation now closed?

- What details were obtained from the police officers requesting the information?

If there is any doubt as to whether information regarding police requests should be disclosed, the IGM / SIGO should be consulted. Enquiries will then be made to establish if releasing the information could prejudice the detection and prevention of a crime.

10.4.8 Datix must be updated with details of any information which is withheld, and the exemptions used.

10.5 Stage four – releasing / withholding the information

10.5.1 As soon as the request has been processed, a standard letter along with the information judged to be the applicant's personal data should be released using the applicant's preferred method i.e. sent via mail, electronically, collection or viewing. All documentation should contain the watermark 'Applicant Copy'.

10.5.2 Should the applicant's preferred format be via email, all information found and attached must be encrypted or protected using another method. The applicant should be advised to contact the Wrexham IG office on 03000 858631 for the password.

10.5.3 Should the applicant's preferred format be via mail, the information must be sent by recorded delivery annotated **'Private and Confidential'**, and packaged securely in a grey polybag. A scanned copy of the recorded delivery reference number should be kept on the shared drive.

10.5.4 If the applicant has chosen to collect the information from a BCUHB office, then a receipt must be signed and photographic ID (e.g. passport or driving licence) provided to confirm the recipient's identity.

10.5.5 If the applicant has chosen, and BCUHB has agreed, to allow the information to be viewed, a member of the IG team will arrange a mutually convenient time and place within 28 calendar days of receipt of proof of ID.

10.5.6 Ideally the viewing should be of photocopied information. Any copies required by the applicant can then be removed as they are being viewed.

10.5.7 If there is no other choice but to view the original record, the process must be witnessed by a member of the IG team to ensure that the applicant is not left alone with the information at any time.

10.5.8 Up to a maximum of one hour will normally be allowed for the applicant to spend viewing the information. However, this time may be extended, if justified, at the IG team member's discretion. The applicant will be informed of the time allowance prior to, and as a condition of, the viewing.

10.5.9 Following release of the information, copies of the original information, the final response, and any withheld / redacted information should be retained.

10.5.10 All copies will be retained for 3 years in accordance with BCUHB's Retention and Destruction Schedule.

10.5.11 If the application has been denied, restricted, or no information has been found, the applicant should be notified in writing using the standard letter and, where appropriate, an explanation of the reasons provided.

10.5.12 All decisions must be recorded on Datix.

11. Dealing with requests from the Police

11.1 There is no legal obligation for BCUHB to disclose information to the Police without a Court Order. However, BCUHB may consider releasing the information under the legislation, without the patient's consent, for the purposes of prevention or detection of crime, or the apprehension or prosecution of offenders. It is mandatory to comply with a Court Order.

11.2 It will be the IGM's / SIGO's decision whether to release information or not. Documentation must be kept detailing how the decision was reached.

11.3 Requests from the Police should be submitted formally in writing, with full details of the data subject, and justification (under Data Protection legislation) for requiring information. It should be counter signed by a senior Police Officer of the minimum rank of Sergeant. Where the information is of a particularly sensitive nature then authorisation must be by an Inspector or above.

11.4 The IGA must log the request onto Datix and forward to the IGM / SIGO to process as soon as possible.

11.5 When the information is ready for release the information must be sent securely.

11.6 If an agreement has been made for the information to be collected, the Police Officer must provide proof of identity e.g. warrant card.

11.7 The date that the information was sent or collected must be recorded onto Datix and a copy of the request form used should be uploaded.

11.8 A copy of the information released should be retained for a minimum of 3 years and the file reference recorded on Datix.

12. Complaints & feedback

12.1 Complaints in relation to the processing and provision of information will be dealt with by the IGM / SIGO and treated as a first internal review.

12.2 Although there is no legal obligation to respond to internal reviews within a specific timeframe, the internal review will be dealt with in line with BCUHB's Putting Things Right (PTR) process which is 30 working days.

12.3 Should the internal review take longer than 30 working days, the applicant should be kept informed of this.

12.4 If the applicant is still dissatisfied with the provision of information, following the internal review of their response, they will be directed to the ICO.

12.5 At their discretion, the IGM / SIGO may decide to conduct one further review of the response if they feel that the matter could be resolved locally.

12.6 Right to rectification

If, following receipt of the response to their subject access request, the applicant feels that any of their personal information is inaccurate they have a right to rectification.

12.6.1 If a request for rectification is received from an individual, these requests must be directed to the IG department BCU.DPO@wales.nhs.uk who will facilitate the request on behalf of BCUHB.

12.6.2 Upon receipt of a request for rectification BCUHB has one month to respond and must take reasonable steps to satisfy the individual that the data is accurate, or to rectify the data if necessary, taking into account the arguments and evidence provided by the individual.

12.6.3 In the event that a correction of factual information is necessary, e.g. misspelt name or incorrect date of birth, it must be obvious who made the amendment and when.

12.6.4 If BCUHB are satisfied that the personal data is accurate, the individual must be informed that BCUHB will not be amending the data, and the reasons why. BCUHB must also inform them of their right to make a complaint to the ICO.

12.6.5 In the event that personal data is found to be inaccurate, all third parties who have received the inaccurate data must be informed of the corrections in writing to ensure that their records are updated accordingly.

12.6.6 BCUHB can refuse to comply with a request for rectification if the request is considered manifestly unfounded or excessive. However, the justification must be recorded and evidenced, and the individual informed of the decision and their right to make a complaint to the ICO.

13. Resources

13.1 The IG team should have sufficient resource in order to assist staff in ensuring BCUHB are compliant against its legislative requirements.

13.2 Departments / Divisions should ensure that their appointed staff have sufficient time and resource in order to execute their responsibilities in complying with SARs in line with legislative timescales.

14. Training

14.1 All staff within BCUHB are mandated to undertake IG training. This training must be renewed every two years.

14.2 Additional training is provided by the IG Team for those staff nominated as IG leads.

14.3 The Information Governance Officers (IGO's) may provide additional ad hoc training sessions for all departments / wards within BCUHB on request.

15. Implementation

15.1 This procedure will be published in line with the Corporate Policy on Policies and awareness is raised via communication channels such as the Corporate Bulletin, Information Governance quarterly Bulletin, staff alerts and IG training.

15.2 Robust controls and auditing processes to be put in place to monitor compliance and manage any incidents with regards to data security breaches.

15.3 Quarterly KPI reports are presented to the Information Governance Group (IGG) with issues of significance reported to the Digital Information Governance (DIG) Committee.

16. Equality including welsh language

16.1 There is no evidence to suggest that this procedure would have a negative effect in relation to race, disability, gender, age, sexual orientation, religion and belief or infringe on the individual's human rights. This will therefore have a positive effect on individuals.

16.2 The IG team have responded to, and applied, the requirements set out within the Welsh Language standards. However, this procedure does not have a negative effect on the Welsh Language as it provides access to information regardless of the language. Forms and leaflets which accompany this Procedure are bilingual, and all correspondence received from an individual will be responded to in the language in which it was received.

17. Well-being of future generations

This procedure has been developed in accordance with BCUHB's well-being objectives and the five ways of working under the Well-being of Future Generations Act 2015.

BCUHB Well-being Objectives:

To improve physical, emotional and mental health and well-being for all;
To target our resources to those with the greatest needs and reduce inequalities;
To support children to have the best start in life;
To work in partnership to support people – individuals, families, carers, communities - to achieve their own well-being;
To improve the safety and quality of all services;
To respect people and their dignity;
To listen to people and learn from their experiences

Five Ways of Working	Evidence
Long Term, Prevention, Integration, Collaboration, Involvement	The purpose of this procedure is to ensure compliance with Data Protection legislation by safeguarding personal data, thus avoiding undue harm or distress to all in the adverse event of a personal data / privacy breach. Also providing a right of access to all who apply for information that is held by BCUHB under Data Protection legislation. It is also aimed at providing assurance that an efficient and robust service / system is in place to comprehensively manage the handling of information and personal data, preventing adverse impact on individuals (distress due to data breaches / loss of confidence) and the organisation (lost revenue due to fines, negative reputational impact) as well as collaborating with staff/multi agency (i.e.police).

18. Environmental impact

There is no environmental impact identified for the implementation of this procedure.

19. Audit

19.1 Every attempt is made to ensure that new policies and procedures, revised policies and procedures are disseminated widely throughout BCUHB. However, all staff must also take responsibility for familiarising themselves with the above on a regular basis. All documents and guidance will be available on the BCUHB intranet site and disseminated via noticeboard announcements, bulletins etc.

19.2 Compliance with this procedure will be subject to periodic review. Any recommendations will normally be implemented after review by the IGG.

19.3 Regular audits to review compliance with the mandated IG training will be carried out to ensure compliance with this procedure.

19.4 Audits will also be carried out by BCUHB's internal audit team.

19.5 BCUHB will respond to the ICO following their audits on how we manage the processing of personal data, control and governance arrangements by measuring and evaluating their effectiveness.

20. Review

This procedure adheres to legislative and statutory requirements and will be reviewed at least every 3 years or sooner if there is a change to legislation.

21. References

The legislation and guidance supporting this policy include but are not limited to:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR) 2016
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records Act 1990
- Access to Medical Reports Act 1998
- Human Rights Act 1998
- Disability Discrimination Act 2005
- Race Relations (Amendment) Act 2000
- Equality Act 2010
- Public Records Act 1958
- Common Law Duty of Confidentiality
- Caldicott Report
- Confidentiality: Code of Practice for Health & Social Care in Wales
- Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the FOIA
- Department of Health Records Management Code of Practice
- WHC (2000) 71 For the Record

Code of Practice on the discharge of obligations of public authorities under the Environmental Information Regulations 2004 (Regulation 16)