GIG CYMRU
NHS WALES

Bwrdd Iechyd Prifysgol
Abertawe Bro Morgannwg
University Health Board

ABMU HB INFORMATION GOVERNANCE PROCEDURES

.

Document Author: Head of Information Governance
Approved by: Executive Team
Approval Date: 13 February 2019
Review Date: 13 February 2021
Document No: HB150

CONTENTS

Page

Please read these Information Governance Procedures in conjunction with the All Wales Information Governance Policy. The IG Policy is a high level national document, and these IG Procedures support the Policy at an operational level within ABMU Health Board.

1. Introduction

ABMU processes a vast amount of patient and staff data and the organisation has a duty to manage that information legally.

The IG Procedures should be followed by all staff, volunteers, students, contractors or anyone else who has access to ABMU's patient and/or staff information. There will be consequences for anyone breaching these Information Governance (IG) Procedures and these may vary depending on the individual circumstances.

2. Aims and Objectives

These IG Procedures supports the corporate objective of embedding effective governance and partnerships.

The aims of these Procedures are to ensure that:

- Staff and patients' personal data is protected from unauthorised access and disclosure;
- All legal, regulatory and professional requirements are met;
- Patients and staff are fully informed about how the personal information they provide will be recorded and used; and
- Appropriate information is provided to the correct person, when it is needed.

3. Definitions

Information Governance (IG) is a framework that defines how organisations and individuals handle information; in particular, both the handling of sensitive and personal information of employees, patients and service users, and also to information related to the business of the organisation.

The use of the term "personal data" relates to the information from which a living individual can be identified, and may refer to patient and/or staff information.

3.1 Personal Data – Patient / Staff identifiable information

Examples of personal data – staff and/or patient – include the individual's name, address, full postcode, date of birth, NHS number, National Insurance number, staff number, local patient identifiable codes as well as photographs, videos, audio recordings or other images**.** Computer IP addresses are also considered personal information, as are certain email addresses. Information which has had identifiers removed or replaced in order to pseudonymise (partially anonymise) the data is still personal data for the purposes of data protection legislation (see section 3.3 for fully anonymised information).

3.2 Special Categories of Personal Data

This is the term used by the General Data Protection Regulation (GDPR) (see section 4) to replace the term "sensitive personal data" used by the Data Protection Act (DPA) 1998. It includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic and biometric data where processed to uniquely identify an individual.

3.3 Anonymised information

This is information which does not identify an individual directly, and which cannot reasonably be used, in combination with other available information from an alternative source, to determine identity. Anonymisation requires the removal of all key identifiable information referred to in 3.1 and any other detail or combination of details that might support identification.

Once information is effectively anonymised, it is no longer confidential and may be used with relatively few constraints. However, it should be noted that in some circumstances an individual might be identified directly or indirectly from other information. For example, rare diseases, drug treatments or statistical analyses, which have very small numbers of patients, within a small population, may allow individuals to be identified. Particular care must be taken in these circumstances to limit access and circulation of the information to minimise the likelihood of the patient being identified inadvertently.

3.4 Processing

Processing refers to how an organisation manages their information and includes its collection, recording, organisation, structuring, storage, adaptation, use, disclosure by transmission, dissemination, restriction, erasure or destruction.

4 Legislative Requirements

The DPA 2018 and the GDPR 2016 came into force in the UK on 25th May 2018. Together they require greater transparency, increased data subject rights (the patient or staff member whose information we are processing) and greater accountability and assurance. This includes:

- The recording of all data processing activities with their lawful justification and data retention periods;

- Assessing the need for a Data Protection Impact Assessment (see section 7.2.1) at an early stage, and incorporating data protection measures by default in the design and operation of information systems and processes;

- Routinely conducting and reviewing data protection impact assessments where processing is likely to pose a high risk to individuals' rights and freedoms;

- Ensuring demonstrable compliance with enhanced requirements for transparency and fair processing, including notification of rights;

- Ensuring that data subjects' rights are respected;

- The provision of copies of records free of charge, rights to rectification, erasure, to restrict processing, data portability, to object, and to prevent automated decision making;

- Notification of personal data security breaches to the Information Commissioner; and

- The appointment of a suitably qualified and experienced Data Protection Officer.

5 Responsibilities

Confidentiality is an obligation for all staff.

Breach of confidence, inappropriate use of or access to health or staff records, inappropriate disclosure of personal data or abuse of computer systems may lead to disciplinary measures being taken (see Information Security Policy for further information). It may also bring into question professional registration and could result in legal proceedings.

All staff, irrespective of access to patient or staff information, need to complete mandatory IG training at induction and then refresh this training every 2 years. Face-to-face training sessions are advertised on the intranet, and e-learning can be accessed via the Electronic Staff Record (ESR) system. Support can be sought from the IG Department if required.

All staff are responsible for proactively identifying IG risk, breaches and near misses, and to report these accordingly (see Section 7.4).

It is the responsibility of all staff to read these Procedures in conjunction with the relevant documents listed in section 10.

5.1 The Board

The ultimate responsibility for IG in the NHS rests with the Board of each organisation, who should note that:

- Information Governance is an important part of the overall governance arrangements for the Health Board (HB);

- IG training is mandatory for all staff; and

- Organisations must provide assurance that they are meeting key IG requirements, including adherence of all staff to these IG Procedures.

5.2 The Chief Executive

The Chief Executive is the Accountable Officer of the HB and has overall accountability and responsibility for IG. He/she is required to provide assurance, through the Annual Governance Statement, that all risks to the organisation, including those relating to information, are effectively managed and mitigated. These IG Procedures are an essential part of the assurance process.

5.3 The Senior Information Risk Owner (SIRO)

The Director of Corporate Governance is the SIRO and is the Board member leading on IG. The SIRO provides an essential role in ensuring that identified information security and IG risks are followed up and incidents managed. The Deputy SIRO is the Chief Information Officer. These IG Procedures provides the framework within which to assess IG compliance and to some extent IG risk across the HB.

5.4 The Caldicott Guardian

The Caldicott Guardian plays a key role in ensuring that the HB satisfies the highest practical standards for handling personal data. Within the HB the Director of Public Health is the nominated Caldicott Guardian and the Deputy Medical Director is the Deputy Caldicott Guardian. The IG Procedures provides the framework for the secure holding and legal sharing of patient information.

5.5 Data Protection Officer (DPO)

The Head of IG holds the role of DPO within ABMU, and is therefore responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. The DPO’s minimum tasks are defined by GDPR (Article 39) as:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;

- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits; and

- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, patients, etc).

It is the DPO's responsibility to instil a robust IG Policy and Procedures within the organisation, to review them regularly, and to monitor compliance with it across the HB.

5.6 Audit Committee

It is the responsibility of the Audit Committee to consider, request appropriate amendments to, and approve the IG Procedures, and to support their implementation across the organisation.

5.7 Information Governance Board (IGB)

The purpose of the IGB is to provide the Audit Committee with evidence based and timely decisions to assist it in discharging its functions and meeting its responsibilities with regard to:

- Information quality and integrity;
- Information safety and security; and
- Appropriate access and use of information (including patient and personal information) to support its provision of high quality healthcare.

The IGB will monitor compliance with the IG Procedures through bimonthly reports received on IG Key Performance Indicators (KPIs) such as incidents which are a clear indication of how well staff are adhering to the IG Policy and IG Procedures.

5.8 IGB Leads

The nominated Leads that represent their SDU/Corporate Department on the IGB will champion these IG Procedures within their areas. They signpost any requests for IG compliance support that they are unable to answer to the IG Department. They have a number of other IG responsibilities that are listed elsewhere and are available on request from the IG Department.

5.9 The IG Lead

The Head of Digital Records and Information Assurance is the IG Lead for ABMU and, as such, promotes the IG Policy and IG Procedures and its compliance across the organisation.

5.10 The Head of IG and the IG Department

The Head of IG is responsible for overseeing the IG systems and processes within the HB and carrying out operational duties for the IG Lead. The Head of IG and the IG Department Team provide expert advice, guidance and training on IG issues and continually monitor the compliance of the HB and its staff against the IG Policy and IG Procedures, whether through audit or on an ad hoc basis.

5.11 Unit Directors and Service Managers

Unit Directors and Service Managers have responsibility for:

- The protection of personal data and for identifying and managing any associated risk;

- Enforcing measures to protect information, including personal data as part of normal/everyday activity, setting and driving forward a culture that properly values, protects and uses data both in planning and delivery of HB services;

- Ensuring that breaches and near misses relating to IG are reported using the HB's IG Incident and Near Miss Procedure (flowchart summary may be seen in Appendix 2);

- Ensuring excellent data quality;

- Having a robust Information Asset Register (IAR) for their areas of responsibility, and for supporting their Information Asset Owners (IAOs) in auditing this and addressing any issues;

- Ensuring a minimum of 95% of staff within their remit area are compliant with their IG mandatory training at all times; and

- Ensuring their staff comply with the IG Policy and IG Procedures.

5.12 All Managers

The responsibilities with regards to IG for all managers are as follows:

- Ensure their staff have read and understood the IG Policy and IG Procedures;

- Ensure their staff have completed IG mandatory training at induction, before being given access to any clinical systems;

- Ensure their staff are released for, and complete, their IG mandatory training every 2 years following induction. This should be monitored monthly and noted during annual performance reviews (PADRs);

- Ensure their staff have appropriate access rights to any information they access;

- Ensure their staff understand that they must not access their own clinical record;

- Ensure their staff understand that consent from a family member, friend or colleague does not give them the right to access that person's record – the only time such a record may be accessed is if it is part of that staff member's normal role and it is in the course of their usual business;

- Ensure their staff are aware of, and adhere to, standards and procedures relating to confidentiality of personal information;

- Ensure that all job descriptions include the standard confidentiality clause;

- Ensure their staff are aware of the legal requirements relating to confidentiality of personal information, which must be met;

- Ensure their staff are appropriately trained in the use of all records management systems relevant to their job;

- Ensure the IG Incident and Near Miss Procedure is followed (flowchart summary may be seen in Appendix 2), any IG breach is reported via Datix within 24 hours, and if serious, immediately inform the IGB Lead and the IG Department;

- Ensure that action plans resulting from IG audits and/or IG breaches are devised and completed; and

- Ensure that the relevant staff passwords to access electronic records systems are immediately disabled if a member of staff leaves the HB's employment.

5.13 All Employees, Contractors, Volunteers, Researchers and Students

All employees, contractors, volunteers, researchers, students or other personnel (paid or otherwise) have the responsibility to comply with the IG Policy and IG Procedures.

All individuals who have access to personal data are responsible for ensuring that any personal data which they hold are kept securely, are not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. This is supported by an appropriate confidentiality clause within their contract of employment.

Any IG incidents or near misses should be reported on the organisation's Datix incident reporting system and reported to the line manager. Staff must be compliant with the IG Procedures, alongside the documents listed in Section 10. Staff must actively participate in the HB's IG induction training and complete further mandatory refresher/update training relating to IG every 2 years.

5.14 Those Who Procure Third Party Contractors

Those who procure outside services must ensure that appropriate contracts and confidentiality agreements are in place with third parties where potential or actual access to the HB's confidential information assets is identified. All contracts must be GDPR compliant and advice may be sought from NHS Wales Shared Services Partnership and/or ABMU's IG Department on this matter. Contractors must formally agree to adhere to the IG Policy and IG Procedures.

5.15 Information Asset Owners (IAOs) and/or Administrators (IAAs)

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared and protected effectively. They have recognisable and manageable value, risk, content and lifecycles. They may be paper, electronic or some other form and may contain personal or non-personal information. It will form part of ABMU's Information Asset Register (IAR).

IAOs are identified as the people who have operational ownership of an information asset, while IAAs are identified as those who are responsible for the day to day management of the asset.

Both IAOs and IAAs are responsible for compliance with the IG Policy and IG Procedures by all staff with access to the Information Assets for which they have responsibility. They are also responsible for the IG components of the assets themselves, such as Data Protection Impact Assessments (see Section 7.21) and Information Sharing Protocols (see Section 7.20.13). They are responsible for annual audits on their assets and for updating the IAR as necessary to ensure current information is available.

6. Compliance with the IG Procedures

Adherence to these Procedures will be monitored by managers, IGB Leads, governance units and the Information Governance Department. Compliance will be monitored informally as well as through other methods such as audits and PADRs. Internal Audit and external bodies such as the Welsh Audit Office and the ICO may also monitor ABMU's overall compliance with these Procedures. Individual breaches, audit results, Subject Access Request compliance and IG training compliance are reported bimonthly to the IGB, and a report received by the Audit Committee.

Any breach of these Procedures must be reported to the appropriate line manager who, when made aware of a breach, must then consider if the matter requires further investigation under the all-Wales disciplinary policy. Advice on how that should be taken forward is available from Workforce Advisors. Additionally, the IG Incident and Near Miss Procedures must be followed (flowchart summary may be seen in Appendix 2).

7. Implementation and Procedural Guidelines

All staff should take advice when required from their IGB Lead or the IG Department – contact details are found in section 9.1.

An IG Handbook containing good practice guidance can be found on the IG intranet pages (link given in section 9.2), also in Appendix 1 (not including contact details; it incorporates Appendix 2 also).

7.1 Keeping personal data physically secure

7.1.1 Staff working with personal data must exercise all reasonable precautions within their working area to protect that information from unauthorised access, misuse, damage or theft. They must comply with existing security procedures so that access to these areas is restricted to authorised staff.

7.1.2 Care must be taken to ensure that manual health records not filed in their usual filing system are formally booked out, tracked and returned as soon as possible after use. When not in file, manual records should be stored closed, in a secure location within the clinical area or office so that neither the demographic label on the outside nor the contents are seen accidentally.

7.1.3 In general, personal records/information should not be taken off HB premises. However, it is recognised that it will be necessary to do so on occasion, for example a patient's personal data will be required on domiciliary or treatment visits outside the HB. For some staff this will be part of their everyday practice due to the nature of the service they provide. In these circumstances, it is the health care professional's personal responsibility to ensure that the security of this information is not compromised in any way. Staff information must be safeguarded in the same manner.

7.1.4 Portable devices, media and paper records must not be left in view in a vehicle during the day, or even in a locked boot out of sight overnight. All information should be kept securely, wherever it is being held. Ideally, all files and portable computers should be kept under lock and key when not in use. Secure boxes or sealed envelopes should be used to transport manual health records (double envelope if particularly bulky).

7.1.5 All correspondence containing personal information must be addressed to a named individual or designated post holder.

Staff should be aware that there may be local procedures in place regarding marking outgoing mail “Private and Confidential” and must check with their local manager.

Further guidance regarding the sending of mail can be found in Appendix 1.

7.2 Disposal of confidential material

All paper material containing confidential and/or personal data must be disposed of appropriately i.e. by shredding or depositing in confidential waste sacks or confidential waste bins. All confidential waste bags must be kept in a secure area not accessible by the public. Removable media such as memory sticks, floppy disks, CDs etc. can be disposed of by contacting IT Security who will advise you on the correct procedures to be followed.

7.3 Keeping personal data electronically secure

7.3.1 Managers must ensure that staff have appropriate access rights to the computer systems necessary to their role. Staff must be compliant with their mandatory IG training before being given access to electronic systems. All users are allocated user accounts and passwords to access these systems and are personally responsible and accountable for the usage of their passwords. The Information Security Policy details the responsibilities of staff in relation to security of information held on the HB's computer systems. All staff who use these systems must comply with the requirements of that policy.

7.3.2 Staff must not access their own ABMU held clinical record.

7.3.3 Staff must not access the ABMU health record of a family member, friend or colleague – even with their consent – unless the access is required as part of the staff member's normal role and it is in the course of their usual business.

7.3.4 All portable computer equipment must be encrypted – see the Information Security Policy for further guidance.

7.3.5 All computer screens must be locked when not in use (Windows key+L, or CTRL+ALT+DEL then ENTER).

7.3.6 Personal mobile telephones should not be used to take photographs of patients – contact Medical Illustration for support. You may however record photo and video on a mobile device registered with the health board mobile device management (MDM) service, within the secure apps provided – please refer to the Mobile Device Policy.

7.4 Incident reporting

7.4.1 Actual breaches of confidentiality, or risks of potential breaches, must be notified to the Line Manager as soon as they occur. Datix must be completed and forwarded to the Clinical Governance Manager or Governance Support Unit, along with the IGB Lead and IG Department – please ensure that the box is ticked that asks if the IG Department need to be made aware of the breach.

7.4.2 The IG Incident and Near Miss Procedure must be followed at all times – this will ensure that the Regulator is appropriately informed and incidents managed accordingly (flowchart summary may be seen in Appendix 2).

7.4.3 Lessons learned from any breach must be put into practice to prevent another breach of the same nature occurring.

7.4.4 The IGB are informed bimonthly of any IG breaches so that assurance can be given that an investigation has been carried out and lessons learned to prevent a recurrence.

7.4.5 In addition, serious breaches of confidentiality occurring outside of normal working hours should be reported to the on-call Manager who will contact the Caldicott Guardian at the earliest opportunity.

7.4.6 The IG Department are solely responsible for informing the Information Commissioner's Office (ICO) of relevant breaches.

7.4.7 The SIRO and/or Caldicott Guardian will consider the requirement to inform Welsh Government of serious IG breaches.

7.5 IG Risk

IG Risks may be noted by any member of staff. If they cannot be immediately solved then they will be added to the appropriate risk register. This may be one or all of the following: SDU/Corporate Department risk registers; the HB IG Risk Register for risks across ABMU; and/or the Corporate Risk Register risks with serious consequences only.

7.6 Fair Processing and Privacy Notices – Informing individuals on the management of their personal data

Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support local clinical audit work to monitor the quality of care provided. It is important that patients are given reassurance that their information will be treated in the strictest confidence at all times by all HB staff who need access to it, that they are informed on what legal basis their information is collected and/or shared, alongside information on rectification, erasure, retention and destruction.

Staff equally have a right to be informed how ABMU manages their information and on what legal basis it is collected and/or shared, alongside information on rectification, erasure, retention and destruction.

Privacy Notices describe how ABMU manages the personal information it holds, and these can be found on its Internet site, for both staff and patients. Leaflets and posters for patients can be accessed for printing from the IG intranet pages (see Section 9.2).

Privacy notices must be created in line with ICO guidance: Using clear and straightforward language, appropriate to the level of understanding for the intended audience, and regularly reviewed to ensure that they are up to date. Templates and guidance for local privacy notices are available on the IG Intranet pages (see Section 9.2).

7.7 Be familiar with the information provided to patients

In order to inform patients properly, staff must themselves be familiar with the content of patient information leaflets, posters and other materials, which deal with confidentiality and the way information is used and shared. Links to these can be found on the IG intranet pages (see section 10.2).

7.8 Check individuals' understanding

Staff must check that patients have had the opportunity to read and understand the information provided, ask any questions they may have and know who to contact for further advice (the DPO or the Caldicott Guardian). It is important to recognise the different communication needs of patients. Difficulty in communicating for whatever reason, such as disability, illiteracy, cultural issues or language difficulties, does not remove the obligation to help people understand.

If staff wish to find out more about how their information is managed, they may choose to contact Human Resources, their line manager or the IG Department.

7.9 Make it clear when information is being noted or accessed

Patients must be made aware that information is being noted and their health records are being accessed. This may require no more than a comment such as "*Let me make a note of that in your file"* and will generally occur naturally as part of the interaction with the patient.

7.10 Good record keeping and data quality

Staff are under a legal obligation to maintain data quality when creating or amending patient and staff records, and should do this in line with professional standards where they exist. The Data Quality Policy should be followed.

In terms of patient records, if a patient requests that an amendment is made to their record then this must be actioned immediately – unless their request refers to a medical opinion or fact in which case advice should be sought from the IG Department as it is usually not possible to change such details unless a mistake has been made on the HB's part. There is advice available from professional bodies, and within ABMU there is a Record Keeping Policy for Nurses.

When information is shared it should be noted in the patient health record or staff record as appropriate. If it is a one-off disclosure, for anything other than the purposes of direct care, then this should be noted on the One-off Disclosure Log which can be found from the SDU Governance Unit, the relevant IGB Lead, the IG Department or the IG Department's intranet pages (see Section 9.2). This One-off Disclosure Log must be copied to the IG Department who keep a central register of all such disclosures.

7.11 Make it clear when information is being disclosed or when it may be disclosed to others

It must be recognised that patients may know little about the NHS and other agencies such as social services and how they work together on a day to day basis. Staff must ensure that patients know when information is disclosed to be used more widely, and how this affects their care

There are certain Acts of Parliament that require disclosure of personal data. Court orders may also require disclosure. Even though the patient cannot prevent disclosure in these cases, they must normally be informed that this is taking place. Further advice can be sought from the IG Department.

7.12 Consent – Check that patients are aware of the choices available in respect of how their information may be used or shared.

Under GDPR the majority of the health information that ABMU processes will fall under Article 9(2h) as its legal basis. This allows processing that is "necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services".

Direct Care is currently defined by Caldicott 3 as "A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care". This is being reviewed on an all Wales basis.

Explicit consent should only be considered as a legal basis for processing if the patient / staff member has a genuine ability to withdraw their consent without it notably compromising the service given by ABMU. Explicit consent is likely to be required if personal information is to be processed outside the remit of Article 9(2h) as described above; advice should be sought from the IG Department.

Implied consent does not give ABMU the ability to share special categories of personal data for reasons other than those mentioned in Article 9(2h) above. Consent under GDPR, when used as a legal basis for processing, needs to be by clear affirmative action on a choosing to opt in rather than opt out basis.

Patients have the right to choose whether or not to agree (consent) to information that they have provided in confidence being used or shared beyond what they understood to be the case when they provided the information, unless there is legal justification or robust public interest basis to do so.

In some cases, it may not be possible to restrict information disclosure without compromising care. This would require careful discussion with the patient, but ultimately the patient's choice must be respected. Where patients insist on restricting how information may be used or shared in ways which compromise the health service's ability to provide them with high quality care, this must be documented in the patient's record.

It must be made clear to the patients that they are able to change their mind at a later stage.

The patient or staff's consent to share their information should be noted in their record. Any lack of consent to share should also be noted and respected. If staff determine information needs to be shared but consent has been refused, then advice may be sought from the IG Department as there may still be a legal basis for sharing. Good practice would state that this was explained with care to the patient or member of staff who had refused their consent.

7.13 The recording of meetings – audio visual or audio only

There is separate guidance available on this matter available on the IG Intranet pages (see Section 9.2). It is essential that no patients, relatives or personal information are recorded inadvertently in the background at any time, and that no patient is recorded without their explicit consent for anything other than their direct medical care – or that of their legal guardian if appropriate.

7.14 Use of information for teaching purposes

Anonymised or dummy information must be used for teaching purposes. It must be emphasised that this principle applies equally to paper-based records, electronic records, recordings and images. Students needing to complete portfolios for their tutors need to anonymise all identifiable information.

7.15 Children and young people

Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment ("*Gillick competent*" children) are those aged 13-15 are also entitled to make decisions about the use and disclosure of information they have provided in confidence. (*They may be receiving treatment which they do not want their parents to know about*). However, where a competent young person or child is refusing treatment for a life threatening condition, the duty of care would require confidentiality to be breached to the extent of informing those with parental responsibility.

In other cases, consent to disclose or share a patient's personal data should be sought from a person with parental responsibility for the child if the information is not being processed for the purposes of direct care of the patient.

7.16 Where patients are unable to give their consent

If a patient is unable to give their consent or communicate a decision due to their physical or mental condition, the health professionals concerned must take decisions about the use of information. This needs to take the patient's best interests and any previously expressed wishes into account. Each situation must be judged on its merits. A record of the patient's incapacity to give their consent must be made in the health record. Only as much information as needed to support their care should be disclosed. In cases where the patient is thought to lack capacity reference must be made to the Mental Capacity Act 2005 – Code of Practice.

7.17 Disclosing information with appropriate care

A duty of confidence arises when one person shares information with another (for example, patient to health professional) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from common law; a requirement established within professional codes of practice and a requirement within HB employment contracts linked to disciplinary procedures.

7.17.1 Identify enquirers

Staff should check that any callers, by telephone or in person, are who they claim to be. Seek official identification or check identity by calling them back using an independent source for the telephone number. Check also that they have a legitimate right to have access to the information. Be aware that some patients may not wish their relatives and/or friends to know that they are on ABMU premises.

Do not give out information to callers, in person or on the telephone, without the consent of the patient. This includes solicitors and usually the police – see Section 7.20.5 for further guidance.

7.17.2 Blaggers

Blaggers are individuals who are paid to gain personal information about patients or staff from the HB illegally. If you are not sure of the identity of the individual making the enquiry do not give them information until you have verified their identity. If you believe that the caller is attempting to gain information illegally you should contact the Counter Fraud Department.

7.18 Share the minimum information necessary

It is important to consider how much information needs to be disclosed before disclosing it. This must be balanced against the need to provide safe care and the consequences of missing information. Providing the whole casenote is generally unnecessary and may constitute a breach of confidence. The seven Caldicott Principles should be followed (Appendix 3).

7.19 Ensure appropriate standards are applied in respect of emails and faxes

Care must be taken to ensure that the means of transferring all personal information from one location to another are as secure as they can be and that they comply with policy. It is preferable to send information electronically following the Information Security and Email Policies, ie. to an email address ending in "wales.nhs.uk", via CJSM, via the Secure File Sharing Portal, via MoveIT, or encrypted. If this is not possible, then the information should be posted or couriered.

If this is not possible, then the last resort is to use a Fax. If personal data is faxed, staff must follow the Fax Policy, confirm that the receiving fax is in a secure location and that receipt of the information will be acknowledged. Information must never be left unattended in a HB fax machine at any time.

7.20 Procedural guidelines for disclosing personal data

Advice can be sought from the IG Department on individual cases whenever required.

Individuals (known as data subjects) have a right to apply for access to information held about them and, in some cases, information held about others. This is known as a Subject Access Request (SAR) and such requests must be made in writing and the information released when appropriate within one month.

7.20.1 Information to patients (Subject Access)

Requests for personal information under the provision of data protection legislation should be directed to the Access to Health Records Department where procedural guidelines are in place to facilitate the process. Information will usually only be shared with someone other than the patient with explicit patient consent or to someone with a Lasting Power of Attorney for Health and Welfare. Occasionally there may be a need to share information without consent due to the presence of a court order (see Section 7.20.10) or other legal reason. Advice should be sought from the IG Department if required.

Any information released must not include reference to a third party unless that 3rd party has also given their consent for the information to be released.

7.20.2 Information to staff (Subject Access)

Requests for personal information under the provision of data protection legislation should be directed to the Head of Workforce Localities and Systems within Workforce and OD where procedural guidelines are in place to facilitate the process. Occasionally there may be a need to share information without consent due to the presence of a court order or other legal reason. Advice should be sought from the IG Department if required.

Any information released must not include reference to a third party unless that 3rd party has also given their consent for the information to be released.

7.20.3 *Information to relatives, carers and others*

Confidential information should only be discussed with relatives or other persons after consent has been obtained from the patient. If it is not possible to obtain consent due to the incapacity of the patient the information must be given in the patient's best interest, taking into consideration any previous direction given by the patient.

Staff must emphasise to the recipient that the information is being given in confidence and ensure that this is fully understood. Patient consent, or inability to give consent along with the recipient's understanding, must be recorded appropriately in the patient's health record.

7.20.4 *Complaints procedure*

Staff must obtain the patient's consent to gain access to their health records in order to investigate a complaint made against the HB. Access is restricted to the information covering the period with which the complaint is concerned. The patient is also required to provide their explicit consent if someone is making a complaint on their behalf.

7.20.5 *Police enquiries*

Information should not be shared with the Police without due consideration for the law alongside relevant ABMU policies and procedures. Staff should refer to the Releasing Information to the Police Procedure, available on the IG Intranet pages (see section 9.2). If further guidance is required, the IG Department should be contacted.

7.20.6 *Common Law and the Public Interest*

Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on an individual case basis, that the public good that would be achieved by disclosing the information outweighs the obligation of confidentiality to the individual patient, and the public interest in the provision of a confidential service.

The terms "serious crime" and "serious harm" are not easily defined. Requests for information, which require such judgements to be made, should be referred to the IG Department.

7.20.7 *Child Protection*

Research and experience has shown that keeping children safe from harm requires professionals and others to share information: About a child's health and development and exposure to possible harm; about a parent who may need help to, or may not be able to care for a child adequately and safely; and about those who may pose a risk of harm to a child.

Professionals can only work together to safeguard children if there is an exchange of relevant information between them. This has been recognised in principle by the courts. Any disclosure of personal information to others must always, however, have regard to both common and statute law.

Normally, personal information should only be disclosed to third parties (including other agencies) with the consent of the subject of that information and wherever possible consent should be obtained. However, in some circumstances, e.g. suspected fabricated or induced Illness, it might undermine the prevention or detection of a crime. Consent may not be possible or desirable in these cases but the safety and welfare of a child must be the first consideration when making decisions about sharing information.

The law permits the disclosure of confidential information necessary to safeguard a child or children in the public interest. That is, the public interest in child protection may override the public interest in maintaining confidentiality. Disclosure should be justifiable in each case, according to the particular facts of the case, and legal advice should be sought in cases of doubt. Advice should also be sought when required from the ABMU Safeguarding team or the IG Department.

7.20.8 Vulnerable Adults

Many of the data protection issues surrounding the disclosure of information in relation to vulnerable adults can be avoided if the informed consent of the individual has been sought and obtained. Consent must be given freely after the alternatives and consequences have been fully explained.

If the information is classified as sensitive, consent to disclose it must be explicit. Particular care must be taken to explain exactly what information may be disclosed and why this is considered necessary.

Informed consent can only be obtained when the vulnerable adult is able to fully understand and participate in the discussion i.e. “has capacity”. Information cannot be disclosed if a vulnerable adult who has capacity refuses to give their consent, as long as there is no risk to others and no crime has been committed.

Where disclosure of information is necessary for the prevention or detection of crime, to protect public safety or to protect the rights and freedoms of others, the law does permit the disclosure of confidential information in the public interest even when informed consent has not been sought, or has been sought and refused. Information shared must always be on a need to know basis and always remain pertinent to the specific situation. In these circumstances, it is important that it is made clear to the alleged victim, and their relatives/carers where appropriate, that in these cases it is necessary for information to be shared with other agencies, such as the police, due to the potential risk to others.

Advice can be sought from the ABMU Safeguarding team.

7.20.9 Medical information for solicitors and insurance companies

In the course of litigation or insurance claim processing, solicitors or insurance companies may request medical information relating to the claim from the patient's health record. It must be established that the person requesting the information is representing the patient for whom medical information is sought and that the patient has given their signed consent to release the information.

Any information released must not include reference to a third party unless that 3rd party has also given their consent for the information to be released. Any such requests are subject to data protection legislation and should be referred to the relevant department.

7.20.10 Court Orders

The courts, some tribunals and persons appointed to hold enquiries have legal powers to require disclosure of confidential information. In the event that a patient's medical details or a member of staff's personal details are required in the course of legal proceedings, a court order may be issued to release information. A formally issued court order directed by a judge or other presiding officer is the only instruction that must be obeyed in these cases. Verbal or written requests from lawyers or court officials are not sufficient.

All such requests for release of information will be dealt with by the relevant department and should be honoured in a timely fashion. A note of exactly what has been released, when and to whom must be made. Copies should be given unless the court order explicitly requests originals.

7.20.11 Deceased patients

Deceased individuals are not covered by data protection legislation. Disclosure of medical information relating to a deceased patient may only be undertaken where the third party who is to receive the information is proven to be the executor of the deceased's estate, held a Lasting Power of Attorney for Health and Welfare at the time of patient's death, or has taken out letters of administration.

Requests from insurance companies for information to process claims will only be fulfilled if they are accompanied by written authority from the executor. Release of information in these circumstances is subject to the requirements of the Access to Health Records Act 1990.

The Access to Health Records Department should be involved in the release of any information relating to deceased patients.

7.20.12 Release of information to the media

During normal working hours any media requests must be directed to the Communications Department who will obtain explicit consent from the person where practicable. Outside these times, requests should be referred to the on-call Manager.

7.20.13 Sharing personal data with others: Information Sharing Protocols (ISPs)

Information Sharing Protocols (ISPs) should provide a framework for the lawful, secure and confidential sharing of information with non-NHS organisations. ISPs should clarify the purposes of why and how personal data is shared and identify the legal basis on which this information is shared, which in turn will help build the good working relationships that lead to trust and effective communication. The IG Department should be informed when an ISP is being considered to enable appropriate support and guidance during its drafting and completion. All ISPs must be checked by the IG Department when complete prior to being signed by the Caldicott Guardian.

The Caldicott Report “Review of Patient Identifiable Information” raised concerns about the management of NHS records, in respect of all patient-identifiable information that passes between NHS organisations, other than for direct care. The Caldicott Principles (Appendix 3) must be followed, and the Caldicott Guardian is responsible for ensuring that these principles are adhered to.

The principles are the basis of good practice in sharing information between teams and across professional and organisational boundaries. They should underpin formal arrangements between organisations where it is necessary to share personal data in order to provide co-ordinated care for individuals.

Personal data may be shared with external organisations in many circumstances, but the framework in place must be followed. Patient clinical care should never be compromised due to IG concerns – if in doubt, please contact the IG Department for advice.

If personal data is regularly shared with external organisations then an ISP should be in place. If it is a one-off disclosure, for anything other than the purposes of direct care, then this should be noted on the One-off Disclosure Log which can be found from the SDU Governance Unit, the relevant IGB Lead, the IG Department or the IG Department’s intranet pages (see Section 9.2). This One-off Disclosure Log must be copied to the IG Department who keep a central register of all such disclosures.

Further information on the governance required for regular external flows of information can be found on the WASPI website (via the IG intranet pages – see section 9.2), or should be sought from the IG Department.

7.21 Privacy by Design – Data Protection Impact Assessments (DPIAs)

All new projects must have IG embedded from the outset. This protects individuals' personal information and provides assurance that ABMU is working to the necessary standards and is complying with data protection legislation. Any IG risks will be identified at an early stage and mitigated against accordingly.

All new projects therefore need to complete a DPIA. The requirement of the documents on the project Lead is the same. ABMU has a DPIA Lead who will provide the necessary support, guidance document and DPIA template – the IG Department should be contacted for details.

7.22 Research

All staff considering research, whether clinical or service improvement, should in the first instance contact the Research and Development Manager to ensure all necessary procedures are followed and privacy by design underpins any project.

7.23 Instant Messaging

Instant messaging is the use of a dedicated application (app) that allows for real time communication between users. Mobile messaging services used by staff must adhere to security and privacy standards. The underlying principles that all staff must abide by are that any personal data held by or in their control must be effectively and appropriately protected against improper access, disclosure and/or loss at all times. Clinicians may also have to defend themselves against regulatory investigation if they have not taken sufficient steps to safeguard confidentiality.

There are three security aspects to consider:

1. Messaging apps may provide adequate levels of end-to-end encryption, i.e. ensuring the security of the data whilst in transit, but whilst at rest the information may be stored in data centres outside the EEA; this breaches national policy. If data is stored outside the EEA it must comply with rigorous standards to ensure it is complies with the security standards required for personal data.

2. Whilst information may be encrypted in transit, it may well sit on a server in its entirety in clear text, where it becomes the property of the app supplier and so users' control over that information is lost.

3. Lastly, there is no formal arrangement between users and messaging providers in respect of processing and storing of any personal data which is a fundamental requirement under GDPR. This is of clear concern with regards to using such apps for business purposes.

Apps such as WhatsApp and Twitter give adequate levels of end-to-end encryption for business communication, but due to the inability for the organisation to comply with all three security aspects above, it is a breach of policy to use such an app for any personal data. Therefore no confidential business, identifiable patient or staff data should be inputted into or transmitted via any such app. This includes text as well as identifiable images or other recordings.

It is essential that, for example, patients are not discussed via any instant messaging system unless the information is truly anonymised with no identifying information, and any pertinent information is replicated into the relevant health record(s) as would be the case with a face to face conversation between professionals. When discussing patients via an app, all participating care team members must be fully confident about the identity of the patient through other means (e.g. telephone call), to avoid potentially life-threatening incidents as a result of mistaking one patient for another.

When using tools such as text messaging, WhatsApp, Viber, Skype and other messaging apps for any business purpose, staff must remember the principles of IG still apply. Some users may have on their ABMU device an NHS Wales install such as Skype-for-Business and/or Cisco Jabber: These have been approved as they are retained within NHS Wales and so all information stays within NHS Wales. This is different to using Skype on a personal or home device as this is not managed within NHS Wales and so is insecure.

For any group messaging activities, group administrators must ensure that:

- Group membership is appropriate for the purpose of the conversation;

- All members recognise their IG responsibilities: particularly when sending messages, e.g. no personal data should be included. Administrators should remind members regularly of this fact;

- Content should be monitored for IG concerns by the Group Administrator(s) and issues must be acted upon immediately – any breach (e.g. use of personal data) must be reported via Datix within 24 hours of becoming aware of that breach (please tick the box that asks if the IG Department need to be made aware) and the IG Incident and Near Miss Procedure followed;

- Groups should be closed when there is no further need for them to remain open;

- The group is being used appropriately and in line with this and other Health Board policies and procedures; and

- Any concerns are voiced to attendees of the group and acted upon appropriately.

As part of local business continuity plans, it may be necessary to establish a WhatsApp group for emergency use only. This is acceptable providing limited personal data is transmitted, and only in a documented emergency situation.

Guidance on the use of instant messaging has been published jointly by NHS England, NHS Digital, Public Health England, and the Department of Health and Social Care – https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-governance-and-technology-resources. It includes the following guidance regarding app usage:

- Ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device's address book;

- If you are an instant messaging group administrator, take great care when selecting the membership of the group, and review the membership regularly;

- Switch on additional security settings such as two-step verification;

- Review any links to other apps that may be included with the instant messaging software and consider whether they are best switched off;

- Separate your social groups on instant messaging from any groups that share clinical or operational information; and

- Unlink the app from your photo library.

The National Cyber Security Centre (NCSC) has published helpful advice on how best to secure your personal device, including advice that is specific to different operation systems – https://www.ncsc.gov.uk/guidance/end-user-device-security. In particular:

- Do not allow anyone else to use your device;

- Set your device to require a passcode immediately, and for it to lock out after a short period of not being used;

- Disable message notifications on your device's lock screen; and

- Enable the remote-wipe feature in case your device is lost or stolen.

Further advice may be sought from the IT Security or the IG Department.

8 References

These Procedures are based on a variety of sources, including current data protection legislation, Confidentiality: Code of Practice for Health and Social Care in Wales, the Caldicott principles, and guidelines from the Information Commissioner's Office. Links to supporting documentation and guidance can be found on the IG intranet pages (see section 9.2).

9 Getting Help

9.1 Contacts:

Senior Information Risk Owner (SIRO)	Director of Corporate Governance
Deputy SIRO	Chief Information Officer
Caldicott Guardian	Director of Public Health
Deputy Caldicott Guardian	Deputy Medical Director
Data Protection Officer	Head of Information Governance Abm.dpo@wales.nhs.uk
IGB Leads	Individuals are named on the IG Intranet site (see section 9.2)
IG Department	Abm.confidentialityissues@wales.nhs.uk
Information Security	itsecurity@wales.nhs.uk

9.2 IG Intranet site:

This can be found by looking on the front page of the Intranet, click on the IT Informatics tab on the top blue bar, click on the Information Governance tab on the right hand side.

http://howis.wales.nhs.uk/sites3/page.cfm?orgid=743&pid=57246

10 Related Policies and Procedures

Policies and procedures are regularly under review. At the time of approval of these IG Procedures, they must be read in conjunction with (all available on COIN on the intranet or by request):

Information Governance:

- All Wales Information Governance Policy
- Information Governance Strategic Direction and Framework
- Information Governance Incident and Near Miss Procedure
- Data Protection Impact Assessment (DPIA) Guidelines
- Information Sharing Protocol Guidelines / Wales Accord for the Sharing of Personal Information (WASPI)
- Releasing Information to the Police Procedure
- Audio Visual Recording Guidance
- Data Quality Policy

Information Security:

- All Wales Information Security Policy
- All Wales Internet Use Policy
- All Wales Email Use Policy
- Fax Policy
- Mobile Communications
- Mobile Device Policy

Health Records:

- Access to Health Records Policy
- Health Records Policy
- Compilation of Health Records Policy
- Retention and Destruction – NHS Code of Practice
- Storage and Security of Health Records Policy
- Health Records Tracking Policy
- Retention and Destruction Policy
- Record Keeping Policy for Nurses

Safeguarding:

- Procedural Response to Unexpected Death in Childhood (PRUDiC) – local ABMU guidance
- Resolution of Professional Differences
- Neglect Guidance Western Bay Safeguarding
- Domestic Abuse Policy Review
- Minor Injuries in Babies Policy
- Disclosure and Barring Policy
- Controlled Access Policy
- Ask and Act Policy Project – Violence against Women, Domestic Abuse and Sexual Violence (Wales)
- WBSCB CPR Enquiries Protocol
- ABMU HB Combined Safeguarding Children Guidance
- Safeguarding Proforma following the Unexpected Death (or near miss) of a Child
- Professional Abuse Policy for Safeguarding Children and Vulnerable Adults
- ABMUHB Interim Policy and Procedure for the Protection of Vulnerable Adults from Abuse
- Good Practice Guidelines for Chaperoning and Intimate Patient Care
- Prevent Strategy Implementation Policy
- Policy for Addressing Staff who are Victims or Perpetrators of Domestic Abuse
- Procedure for the Management of Fabricated or Induced Illness
- Policy for Health Professionals on Female Genital Mutilation

Communications:

- Social Media Guidance

- Social Media Policy
- Do you want to use social media for work purposes?

Other:

- Security Policy
- Telephone Use Policy
- Decommissioning and Disposal Policy
- Mental Capacity Act 2005 – Code of Practice
- Research and Development Operational Framework
- Risk Management

Appendix 1

Information Governance (IG) Handbook

Visit the IG Intranet Pages for More Information

Report all IG Breaches onto Datix within 24 hours as there is a legal requirement for this. Failure to do so may result in a fine to ABMU of £23 million. DO NOT DELAY!!

- **General:**
  - Follow the "Information Governance Policy" and "Information Security Policy" (available on the Intranet or contact the IG Dept).
  - Always ensure that health records, staff records and any other personal/confidential information are secure when you leave the office/nurses' station etc..
  - Lock rooms or cupboards where personal (staff and patient) data is stored when an area is unmanned.
  - Ensure personal data cannot be seen through windows, in reception areas, in consulting rooms, etc..
  - Do not access clinical systems for reasons not directly work related: This breaches Policy and could result in your dismissal. This includes your own records and those of colleagues, family and friends, even with their consent. The only exception to this is if you are involved in their care, including admin staff involved in arranging care.
  - Treat personal information as if it is your own.
  - Never leave records, sensitive information or electronic devices unattended and in view in a vehicle.
  - Do not post online comments that are offensive or breach confidentiality on social networking sites.
  - Remove any confidential information from printers and fax machines once printed/sent/received.
  - Ensure papers containing personal information are destroyed appropriately – shred or use confidential waste sacks/bins.
  - Let your patients know how we use and manage their information: Posters and leaflets are available to download on the IG intranet pages (IT Informatics tab on Intranet front page, then Information Governance).
  - Tell the IG Department if you have your own departmental information that you give patients (unless they are purely clinical which we do not need to review) or staff, including leaflets, letters, posters or newsletters so we can review them for legal compliance.
  - Follow the Decommissioning Policy if you are moving offices, buildings or disposing of old equipment or furniture. Ensure no personal data is left in unexpected places, e.g. piece of paper under a mattress.
  - If you share personal data externally with a non-NHS organisation regularly, please advise the IG Dept
  - If you share patient information externally, please note this in the patient record – what/why/when/who with.
  - Do not enter into local contracts without Procurement support – they may not be legally compliant.
  - If you are responsible for a new project, or a major new information flow, there is a legal requirement to complete a Data Protection Impact Assessment – email abm.confidentialityissues@wales.nhs.uk for details.
  - Use your IGB Lead as your first point of contact for IG queries (see contacts section for details).
  - Contact your IGB Lead if you identify any area of IG risk so they can add it to the relevant Risk Register.
  - Ensure the Information Asset Register (IAR) includes details of all information held on databases, spreadsheets, documents, paper records stored offsite, locally in filing cabinets, etc – anything necessary for your department's business to take place needs to be logged. Email the IG Dept or your IGB Lead for details.
- **Telephone and face-to-face good practice:**
  - Speak discretely at all times – in consulting rooms, on the wards, in the corridors etc..
  - Only share personal information via telephone when you have confirmed the caller is authorised to receive it.
  - Remember the Caldicott Principles and the 'need to know' principle when discussing patients.
  - Don't gossip.
  - Be careful of how much information you leave on answering machines or voicemail.
- **Communication with the Police:**
  - Unless this is a regular part of your job, contact the IG Department for further advice. There are procedures available for release of information to the Police (ask the IG Department or visit the IG pages on the Intranet).

- **PC good practice:**
  - Follow the “Information Security Policy”, “E-mail Use Policy” and “Internet Use Policy” (available on the Intranet or contact the IG Department).
  - No personal IT equipment is allowed to connect to the Health Board network. However, you may connect your own equipment to the free WIFI service provided by Sky in your own time, and use Mobile Iron to access work data.
  - Always save work to a secure network drive and not to the c: drive or the desktop.
  - Lock or log out of workstations when unattended (Ctrl+Alt+Delete, then the enter key OR Window key+L**)**.
  - Do not share or pass on your password - keep it private.

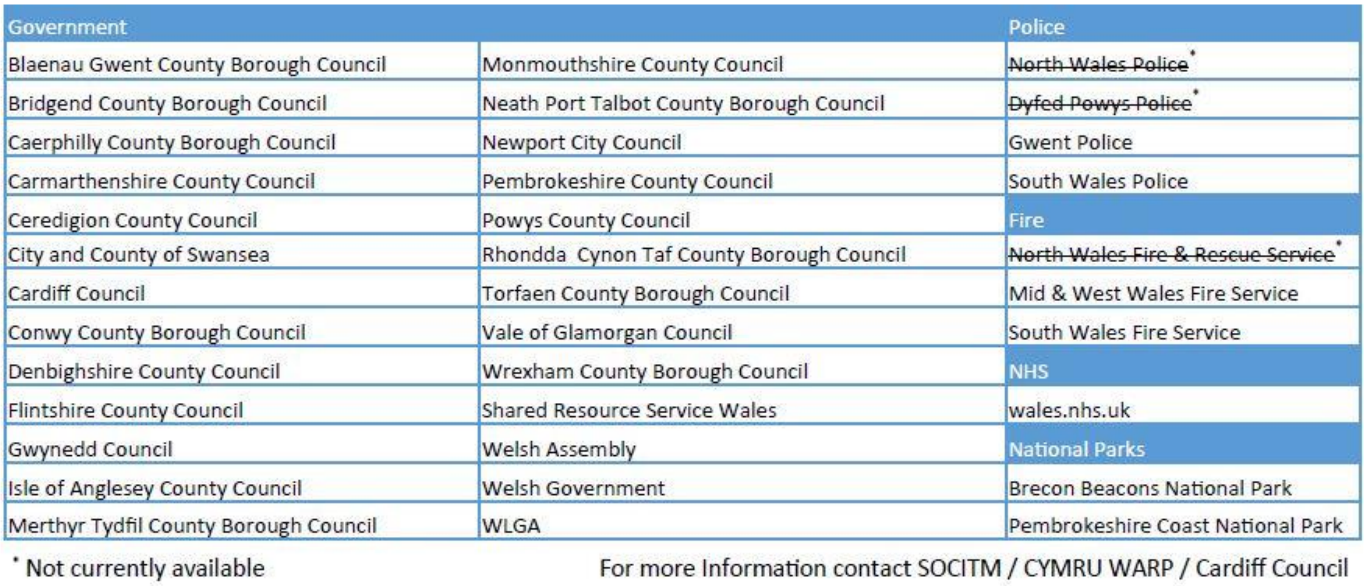
- **Sending of Mail:**
  - Please double check the address you are using with the most up-to-date information available. If you notice a discrepancy please don't guess - find out which is the correct address and organise to have the incorrect address(es) updated immediately.
  - If you are handwriting an envelope, write neatly and clearly and include the recipient's full name and address.
  - If you are using a window envelope, ensure that only the name and address of the recipient is visible through the envelope when sealed (shake it if necessary to check the letter doesn't shift position).
  - Consider the use of “Private and Confidential” on the envelope – departments should make their own decisions, weighing up the risk of flagging the envelope as containing potentially sensitive information to those other than the recipient, versus the benefit of stating the envelope is private. You may choose to mark the envelope as “For addressee only” instead.
  - Use two envelopes if sending anything heavy or bulky.
  - Ensure all envelopes are fully sealed, but do not use any Sellotape on an envelope as this can lead to it sticking to a letter to be sent to someone different by mistake (this has happened and the Information Commissioner’s Office recommended no Sellotape use).
  - If hand delivering a letter, ensure that the envelope has still been fully addressed with the recipient's name and address, and ensure that it is handed over to the recipient only or posted through the correct secure letterbox.
  - Consider the need to use a courier service, or tracking and/or 'signed for' services through Royal Mail, to ensure confidentiality and audit of the delivery and receipt of the letter/package.

- **Faxes**
  - Follow the Fax Policy (available on the Intranet or contact the IG Department).
  - Make sure you have the correct fax number and that there is an appropriate person ready to receive the fax at the other end.
  - Emailing within policy is preferable, followed by the Secure File Sharing Portal, MoveIT or CJSM (ask the Information Security Manager for details), then Royal Mail or internal mail ….. fax as a last resort only.
  - Check and check again.

- **<u>Transfer of personal data – patient and/or staff – via e-mail</u>**

  Personal data is information relating to an individual, including their image or voice, which enables them to be uniquely identified from that information on its own, or from that and / or other information available. Personal data refers to patient or staff information. The transfer of personal data via e-mail should be controlled as follows:
  - **Within NHS Wales (addresses ending in wales.nhs.uk) -** Personal data can be sent anywhere within the Welsh NHS network (wales.nhs.uk) without password protection or encryption. This includes GPs at their wales.nhs.uk address, as long as the process has been agreed with them first.

  - **Within Public Sector in Wales** - Following work undertaken by a number of Welsh public sector organisations and NHS Wales, e-mails will be automatically encrypted in transit between ourselves and the organisations listed here:



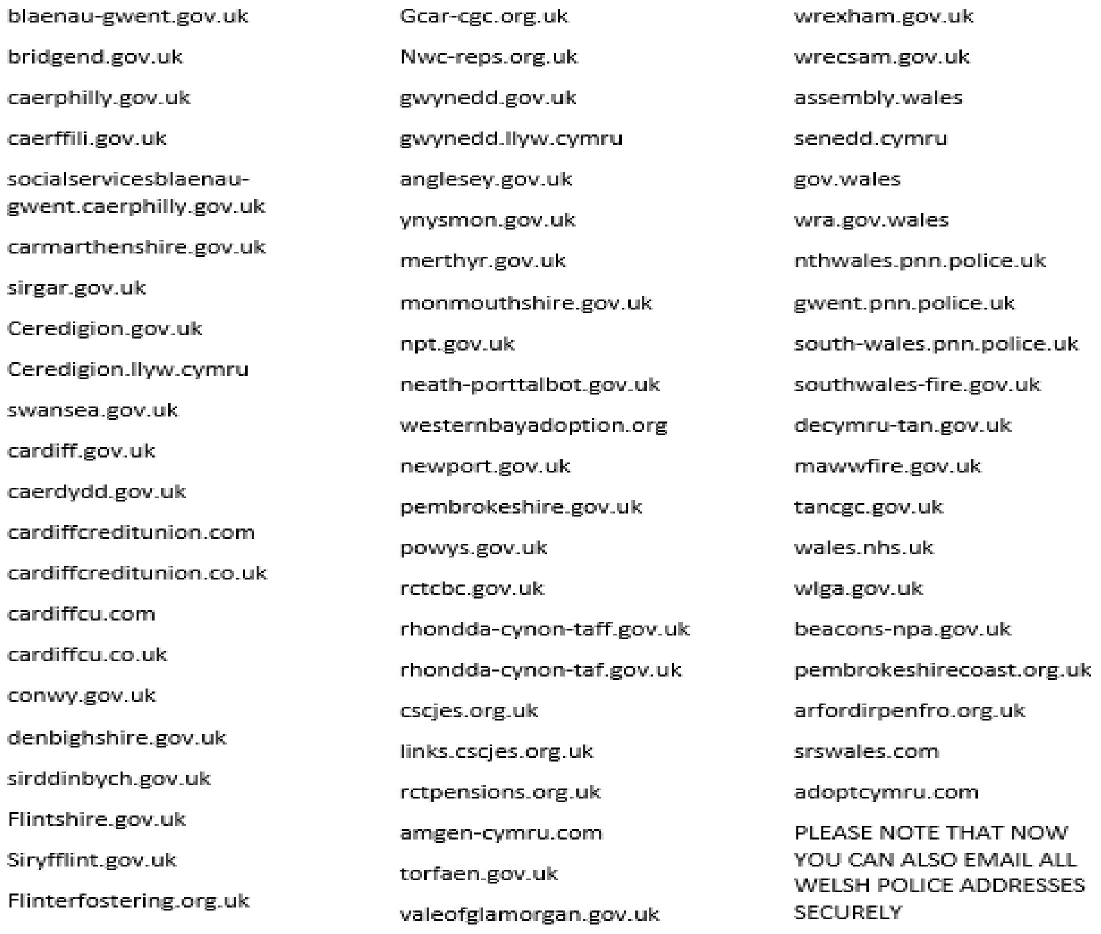
Government		Police
Blaenau Gwent County Borough Council	Monmouthshire County Council	~~North Wales Police~~*
Bridgend County Borough Council	Neath Port Talbot County Borough Council	~~Dyfed Powys Police~~*
Caerphilly County Borough Council	Newport City Council	Gwent Police
Carmarthenshire County Council	Pembrokeshire County Council	South Wales Police
Ceredigion County Council	Powys County Council	Fire
City and County of Swansea	Rhondda Cynon Taf County Borough Council	~~North Wales Fire & Rescue Service~~*
Cardiff Council	Torfaen County Borough Council	Mid & West Wales Fire Service
Conwy County Borough Council	Vale of Glamorgan Council	South Wales Fire Service
Denbighshire County Council	Wrexham County Borough Council	NHS
Flintshire County Council	Shared Resource Service Wales	wales.nhs.uk
Gwynedd Council	Welsh Assembly	National Parks
Isle of Anglesey County Council	Welsh Government	Brecon Beacons National Park
Merthyr Tydfil County Borough Council	WLGA	Pembrokeshire Coast National Park

* Not currently available

For more Information contact SOCITM / CYMRU WARP / Cardiff Council

This means that we can now send identifiable and confidential information securely between ourselves and these public sector organisations. Please remember that we must still be vigilant and ensure the e-mail address we are sending the information to is correct and that we have a legal reason for sharing this information under the Data Protection Act 2018 (GDPR). For further information please contact the Information Security Manager, ext. 43650.

Regarding the security of e-mail between NHS Wales and a number of other public bodies, it is now as safe to send mail between ourselves and these organisations as it is to other NHS Wales e-mail addresses. Please see if the address you want to email Person Identifiable Details ends with following domain, @:



blaenau-gwent.gov.uk
bridgend.gov.uk
caerphilly.gov.uk
caerffili.gov.uk
socialservicesblaenau-gwent.caerphilly.gov.uk
carmarthenshire.gov.uk
sirgar.gov.uk
Ceredigion.gov.uk
Ceredigion.llyw.cymru
swansea.gov.uk
cardiff.gov.uk
caerdydd.gov.uk
cardiffcreditunion.com
cardiffcreditunion.co.uk
cardiffcu.com
cardiffcu.co.uk
conwy.gov.uk
denbighshire.gov.uk
sirddinbych.gov.uk
Flintshire.gov.uk
Siryfflint.gov.uk
Flinterfostering.org.uk

Gcar-cgc.org.uk
Nwc-reps.org.uk
gwynedd.gov.uk
gwynedd.llyw.cymru
anglesey.gov.uk
ynysmon.gov.uk
merthyr.gov.uk
monmouthshire.gov.uk
npt.gov.uk
neath-porttalbot.gov.uk
westernbayadoption.org
newport.gov.uk
pembrokeshire.gov.uk
powys.gov.uk
rctcbc.gov.uk
rhondda-cynon-taff.gov.uk
rhondda-cynon-taf.gov.uk
cscjes.org.uk
links.cscjes.org.uk
rctpensions.org.uk
amgen-cymru.com
torfaen.gov.uk
valeofglamorgan.gov.uk

wrexham.gov.uk
wrecsam.gov.uk
assembly.wales
senedd.cymru
gov.wales
wra.gov.wales
nthwales.pnn.police.uk
gwent.pnn.police.uk
south-wales.pnn.police.uk
southwales-fire.gov.uk
decymru-tan.gov.uk
mawwfire.gov.uk
tancgc.gov.uk
wales.nhs.uk
wlga.gov.uk
beacons-npa.gov.uk
pembrokeshirecoast.org.uk
arfordirpenfro.org.uk
srswales.com
adoptcymru.com

PLEASE NOTE THAT NOW YOU CAN ALSO EMAIL ALL WELSH POLICE ADDRESSES SECURELY

- **Outside Public Sector in Wales -** The transfer of personal data via e-mail outside of the Public Sector in Wales is not permitted **unless** it is contained within an encrypted attachment/document. This would include e-mail to such recipients as English NHS organisations. However, if personal data must be sent to these recipients then please contact the Information Security Manager for advice, ext. 43650.

[The IG Handout has a list of contacts on it and this is kept current before circulating at training sessions. For the purposes of these IG Procedures, contacts are kept up to date on the IG Intranet pages – and include details for the Data Protection Officer, IG Department, FOIA Department and IGB Leads.

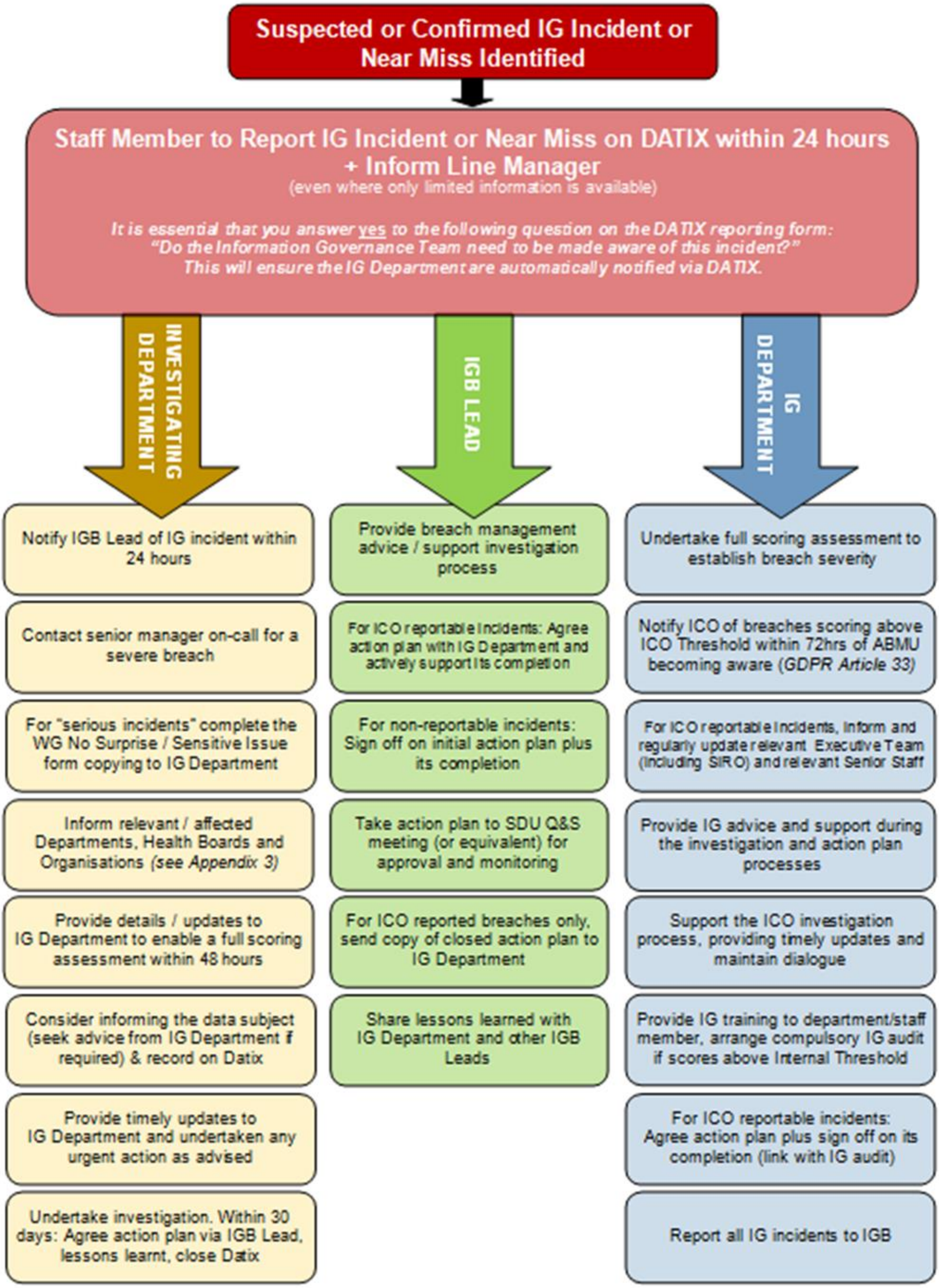
Training is mandatory and must be updated once every 2 years. Training is available through general Health Board sessions advertised via the Intranet and e-mail, or by Departmental visits by a member of the IG Department. Email abm.confidentialityissues@wales.nhs.uk for details. There is e-learning available (details available on the Intranet site – go to the IT Informatics tab, then Information Governance), but we strongly recommend you attend a face-to-face session at least every other refresher, i.e. every 4 years.

Short term placements such as students or agency staff should attend a face to face session if possible, but if not, then they MUST read the IG Intranet Pages and sign the confidentiality agreement via the link on the IG intranet pages to be kept on file by the relevant department.

[The IG Handout includes the IG Incident Flowchart also, this can be seen within this IG Procedures document at Appendix 2].

The IG Handout is updated regularly so please check the IG Intranet pages for the most up to date version. Thank you.

IG Incident Flowchart



Suspected or Confirmed IG Incident or Near Miss Identified

Staff Member to Report IG Incident or Near Miss on DATIX within 24 hours + Inform Line Manager
(even where only limited information is available)

It is essential that you answer yes to the following question on the DATIX reporting form: "Do the Information Governance Team need to be made aware of this incident?" This will ensure the IG Department are automatically notified via DATIX.

INVESTIGATING DEPARTMENT

- Notify IGB Lead of IG incident within 24 hours
- Contact senior manager on-call for a severe breach
- For "serious incidents" complete the WG No Surprise / Sensitive Issue form copying to IG Department
- Inform relevant / affected Departments, Health Boards and Organisations *(see Appendix 3)*
- Provide details / updates to IG Department to enable a full scoring assessment within 48 hours
- Consider informing the data subject (seek advice from IG Department if required) & record on Datix
- Provide timely updates to IG Department and undertaken any urgent action as advised
- Undertake investigation. Within 30 days: Agree action plan via IGB Lead, lessons learnt, close Datix

IGB LEAD

- Provide breach management advice / support investigation process
- For ICO reportable Incidents: Agree action plan with IG Department and actively support its completion
- For non-reportable incidents: Sign off on initial action plan plus its completion
- Take action plan to SDU Q&S meeting (or equivalent) for approval and monitoring
- For ICO reported breaches only, send copy of closed action plan to IG Department
- Share lessons learned with IG Department and other IGB Leads

IG DEPARTMENT

- Undertake full scoring assessment to establish breach severity
- Notify ICO of breaches scoring above ICO Threshold within 72hrs of ABMU becoming aware *(GDPR Article 33)*
- For ICO reportable Incidents, Inform and regularly update relevant Executive Team (Including SIRO) and relevant Senior Staff
- Provide IG advice and support during the investigation and action plan processes
- Support the ICO investigation process, providing timely updates and maintain dialogue
- Provide IG training to department/staff member, arrange compulsory IG audit if scores above Internal Threshold
- For ICO reportable incidents: Agree action plan plus sign off on its completion (link with IG audit)
- Report all IG incidents to IGB

Appendix 3

Caldicott Principles

- **Justify the purpose(s).**

  Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate Guardian.

- **Don't use patient-identifiable information unless it is absolutely necessary.**

  Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

- **Use the minimum necessary patient-identifiable information.**

  Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

- **Access to patient-identifiable information should be on a strict need-to-know basis.**

  Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

- **Everyone with access to patient-identifiable information should be aware of their responsibilities.**

  Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- **Understand and comply with the law.**

  Every use of patient-identifiable information must be lawful.

- **The duty to share information can be as important as the duty to protect patient confidentiality.**

  Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.