ABMU AUDIT COMMITTEE	
Main Report	Audit Committee Meeting On : 23rd January 2018 Agenda item: 2a
Subject	Information Governance Board December 2017: Summary of the key decisions, issues and matters for Audit Committee
Prepared & Presented by:	Sian Richards, Head of Digital Records and Information Assurance
Approved by	Hamish Laing, Executive Medical Director & CIO

1. Purpose

To inform the Audit Committee of significant matters from the Information Governance Board (IGB) meeting of 13th of December 2017. The full minutes and papers of the meeting are available on request.

Background

The Information Governance Board (IGB) provides oversight and direction for Information Governance and provides the Health Board with the assurance that effective information governance is in place. The IGB is chaired by the Senior Information Risk Owner (SIRO), Hamish Laing, Executive Medical Director.

2. Key Decisions and Issues Considered by IGB

The Audit Committee are asked to note the following main areas discussed and agreed at the December 2017 IGB.

3.1 Caldicott Principles into Practice (C-PiP) Assessment

The final annual Caldicott Principles into Practice (C-PiP) assessment was **received** by IGB. ABMU achieved 89% compliance, up notably from the 2015-16 score of 78.5%. This reflects progress made across the Health Board in areas such as the establishment of the IGB and Leads, the SIRO, the appointment of Head of IG, the IG Strategic Framework, the IG Risk Register, the development of an Information Asset Register, the IG audits, the implementation of systems access monitoring of (NIIAS) and overall tightening up of IG processes across ABMU.

3.2 IG Risk Register

IGB **received** the risk report with an updated Health Board IG Risk Register. There are 20 risks on the IG Risk Register. It was **agreed** to establish an IGB Risk subgroup to ensure robust management of risks and their mitigation. IGB **agreed** that the risk in relation to the Health Board readiness for General Data Protection Regulation (GDPR) (see below) should be escalated to the corporate risk register. It was **noted** that IG training and IG resources have already been escalated to the corporate risk register.

3.3 General Data Protection Regulations (GDPR) Positon Statement

The GDPR comes into force on 25th May 2018 as law in the UK. It will replace the Directive that is the basis for the UK Data Protection Act 1998, which will be repealed or amended. It is expected that the provisions of the GDPR will remain in force post-Brexit, and for the foreseeable future.

Although general principles of data protection remain similar, there is greater focus on evidence-based compliance, with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance – up to 4% of turnover per breach which may be imposed for any infringement of the Regulation, not just data security breaches. The more challenging requirements of GDPR are long-term not just transitory.

The GDPR introduces a principle of *'accountability'*. This legally requires that organisations must be able to *demonstrate compliance*. The key obligations to support this include:

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

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

- Assessing the need for data protection impact assessment at an early stage, and incorporating data protection measures by default in the design and operation of information systems and processes

- 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 *within 72 hours* of knowledge of the breach occurring, and for the investigation to be fully completed and reported upon within a few weeks

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

ABMU have completed an All Wales readiness position statement on GDPR for the Wales Information Governance Board (WIGB). The Information Governance team have also completed an internal detailed gap analysis and action plan. The outcome of both pieces of work is that is that ABMU **does not expect to be compliant with the law from May 2018**.

The reasons for predicting non-compliance by May 2018 are detailed in the IGB paper. Insufficient resources available to the IG team have prevented delivery of a plan to meet all the requirements in time. Welsh Audit Office identified that levels of IG resourcing would render ABMU as not being able to adequately prepare for GDPR implementation by May 2018 in their feedback on a recent audit. The ICO have also formally noted that the resources are too poor to enable GDPR compliance within ABMU. The ICO has recommended, as a minimum, the need for IG Assurance Officers under GDPR whose roles would be to focus in particular on auditing systems and processes, training, practice and contracts.

IGB **agreed** that an options paper be presented to the Executive Team in December, noting the Health Board's predicted non-compliance and seeking support for additional resources to be allocated. Executive Team recommended that a proposal be considered by the Investment and Benefits Group in January 2018. It is noted that under GDPR there is an ongoing need to maintain standards, the work required is not a one off exercise. Additional resources will be required to

maintain standards and ensure a continued GDPR compliance to mitigate against penalties and poor IG practices. Executive Team **agreed** for temporary additional support to be appointed, pending consideration of the substantive proposal to permit greater compliance by May 2018 and reduced risk to the organisation.

The Health Board will receive in the January meeting a report that advises them on ABMU's current readiness for the introduction of GDPR and an overview of the NIS Directive, a copy of the paper is available in **Appendix 1** for information.

Audit Committee will be updated on progress and ABMUs status in relation to GDPR.

3.4 IGB Leads Update

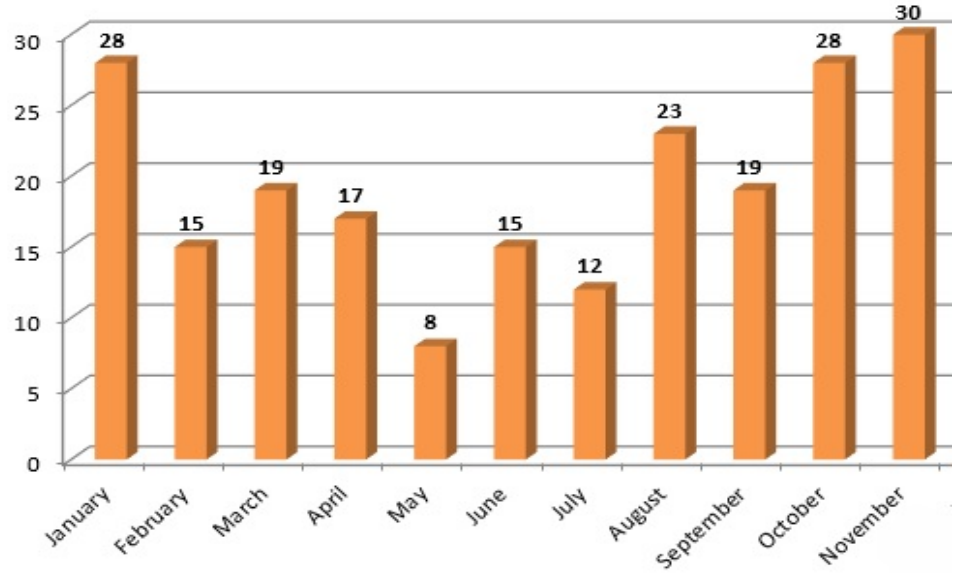
IGB **received** comprehensive reports from each of the SDU and corporate IGB leads on the progress and development of IG practices in their areas. Information included progress in relation to training, risk management, Information Assets Register and incident management. The updates demonstrated the breadth of work that the leads are undertaking to improve the management of IG in the Health Board. The model of identified IG leads in each unit is maturing well and is a good indicator of the progress of the IGB in the last 12 months. Full reports by area are available on request.

3.5 Performance Indicators

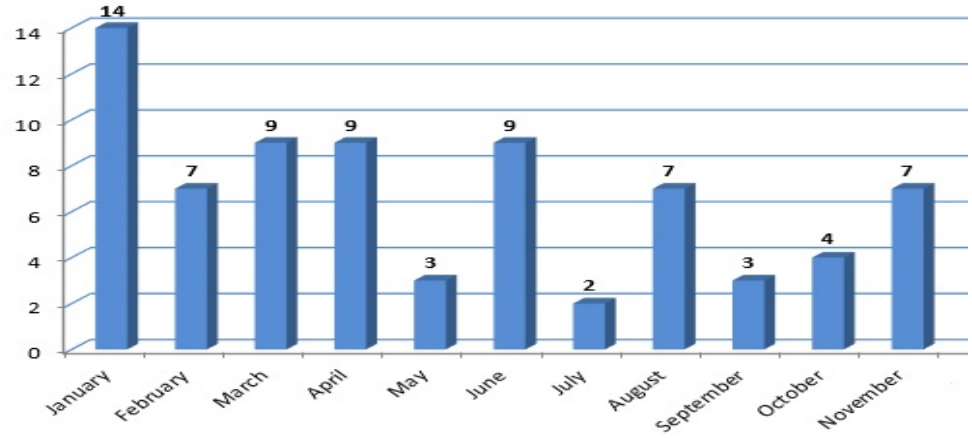
The following performance indicators were **discussed** at the IGB meeting

National Intelligent Integrated Audit System (NIIAS)
NIIAS is a software auditing tool available to all Health Boards / Trusts across NHS Wales. It is used to detect potentially inappropriate access to electronic clinical records where employees may have accessed and/or viewed data they are not entitled to access. Since August 2016 alerts are being evaluated once a week for the previous 7 days. This retrospective monitoring is currently concentrating on two alert scenarios; Access to own record and Access to family record (person with the same surname residing at the same address). The update to IGB reported the number of NIIAS breaches as follows

Own Record (since January 2017)



Family Record (Since January 2017)



There has been a disappointing rise in access to Own Record during October & November, with November being the highest total of the year so far (30). Monthly reports from the IG Department NIIAS Incident Access database are now being sent to the IGB Leads from each SDU / Directorate. Full breakdown by SDU/ corporate department is available in the IGB papers. Each potential breach is subject to individual investigation and disciplinary action if appropriate.

IG Training

IGB **received** a report on completion of Mandatory Information Governance (IG) training across the Health Board. Overall IG training compliance of **58%** was reported for the period up to September 2017, an improvement of **6% since September 2017** and up **25% from January 2017**. Whilst the improvement was recognised, IGB Leads were requested to accelerate IG training in their areas with an aim to reach and maintain the 95% target. IG Awareness Training is part of ABMU's mandatory training and core skills framework. It should be completed by all staff at Induction via e-learning and then refreshed every 2 years, preferably via face-to-face delivery. If e-learning is completed then staff should complete their next training via face-to-face as this covers all local policies whereas e-learning is all-Wales and very high level only. Open access training is offered around the Health Board sites every month, advertised via the IG Intranet site, bulletins and emails. In-house departmental training is available on request, but there has been a drop in the number of Departments requesting such training. The table below shows compliance by SDU/Corporate Department:

Area	**Number of staff in area @ 01.12.2017**	**Compliance % as it stands on 01.12.2017** **COLOUR CODING:** **Green = 95-100% compliance** **Yellow = 75-94% compliance**	**Movement from last IGB Reported Compliance % (@ 04/09/2017)**

		Red = 0-74% compliance	
Corporate Departments			
Board Secretary	46	67	+16
Clinical Medical School	19	53	+5
Clinical Research Unit	39	82	/
Delivery Unit	34	82	-4
Director of Strategy	1653	29	+3
Director of Therapies & Health	28	75	+10
EMRTS	28	75	+37
Finance	91	96	+4
Informatics	386	95	+1
Medical Director	49	94	+5
Nurse Director	77	83	+11
Workforce	124	88	+21
SDUs			
Mental Health & Learning Disability	2027	70	+4
Morriston Hospital	3627	49	+5
NPTH	1428	72	+8
Primary Care and Community	1749	73	+9
Princess of Wales Hospital	1784	63	+8
Singleton Hospital	2374	49	+6
TOTAL			
Overall Health Board	15563	**58**	+6

IG Incident and Breaches

Health Board have been waiting for the outcome impact and potential monetary sanctions of two incidents that were reported to the Information Commissioners Office (Hunter Street and Landauer). During the period it was confirmed by the ICO that these incidents would not incur a financial penalty and were now closed.

There is currently another incidents that is awaiting an ICO decision, which is a patient complaint in relation to the availability of their maternity records**.** This incidents will be monitored accordingly and progress reported back to the IGB.

Subject Access

The Data Protection Act 1998 gives every living person the right to find out what information is being held on computer and in manual records. This is known as 'a right of subject access' and it applies to all health records. The report highlighted the continued good compliance with the Subject Access Request process under the Data Protection Act, achieving compliance of **99.97%.**

In September and October there were 15 reported incident of the Subject Access team finding misfiled information in the Health Record. This figure equates to **1.62%** of the total number of records that were requested during this period. All Health Records and Clinical Coding staff will continue to raise Incident forms to ensure poor records management practices and potential breaches of patient confidentiality are highlighted, in order that these practices can be investigated and eradicated.

3. Policy Approval

Health Records Policy

IGB **noted** that the overarching Health Records Policy is due for renewal at the end of January 2018, however it is expected that Welsh Government will release an All Wales Policy early in 2018 that will supersede the Health Board's policy. The Health Records Department therefore requested that the current 'live' Health Records Policy is extended for a further 12 months until January 2019 to allow for the All Wales policy to be published. IGB **approved** this extension as the policy is still relevant and up to date.

Audit committee are to ratify to the extension of the policy to allow for the All Wales policy to be published.

Police Disclosure Procedure

IGB **received** the procedure that had been developed in partnership with South Wales Police and a multidisciplinary group across ABMU (**appendix 1)**. This procedure provides advice and guidance to staff on handling requests from the Police for personal information that might be required as evidence, or for investigation. The procedure describes the steps that staff should follow before any information is released and addresses a significant gap in guidance currently available to staff.

Audit committee are asked to approve the above procedure.

4. Recommendation

Audit committee are requested to note the summary report from the IGB in December and ratify the Police Disclosure Procedure and the decision to extend the Health Records policy.

Releasing Information to the Police Procedure

1. Background

All Health and Care staff should, to the extent permitted by law, support other parts of the public sector, including the police, in their work. This can include the provision of personal information about service users or staff but there are legal constraints on what can and should be provided depending upon the circumstances.

Personal information should not normally be given to anyone about an individual, including the Police, without that individual's explicit consent, including information relating to the deceased. However under certain legal circumstances, the common law duty of confidentiality can be overlooked and personal information released. Information may be released about a single individual or a larger group of patients or staff as a result of an incident. Information may be released following a direct request from the Police or where the Health Board has deemed it appropriate to share the information in the public interest or for the prevention or detection of crime.

This procedure will provide advice and guidance to staff on how to handle requests from the Police for personal information that might be required as evidence or for investigation, and the procedure that needs to be followed before any information is released.

2. Legal Scope of Requests

Although not exhaustive, the following list details the legislation under which the Health Board might normally receive requests for personal information from the Police (and other authorised bodies):

- Section 29 (Crime & Taxation) of the **Data Protection Act 1998**
- **Section 35 (Court Order) of the Data Protection Act 1998**
- Codes B & D of the **Police & Criminal Evidence (PACE) Act 1984**
- **The Proceeds of Crime Act 2002**
- **The Children's Act 2004**
- **The Misuse of Drugs Act 1971**
- **The Road Traffic Act 1988**
- On request of the **Coroner**
- Section 136 of the Mental Health Act
- Terrorism Prevention and Investigation Measures Act 2011
- **NHS Counter Fraud investigations** Under the NHS Act 2006, investigations into fraud in the NHS may require access to confidential patient information. The investigators have the power to require the disclosure of the relevant parts of a patient's record, should they believe that this is important to the investigation.

2.1. Legal Duty to Disclose (you MUST disclose)

There are circumstances where a disclosure is required by law. The Police request should state what legal basis they are relying on or what Act they are making the application under. Common examples include:

Prevention of Terrorism Act (1989) and Terrorism Act (2000). Staff MUST inform the Police if you have information (including personal information) that may assist them in preventing an act of terrorism, or help in apprehending or prosecuting a terrorist.

The Road Traffic Act (1988). Staff have a statutory duty to inform the Police, when asked, of any information that might identify any driver who is alleged to have committed an offence under the Act. You are not required to disclose clinical or other confidential information.

The Female Genital Mutilation Act (2003). You have a statutory duty to report to the police under Section 5B of this Act where it appears that a girl under the age of 18 has been subject to genital mutilation.

Court Orders Section 35 of DPA are also sometimes obtained by the Police to acquire information from organisations or individuals. Staff should always seek advice from senior managers and legal advisors/medical defence organisations where a Court Order has been served. Where a Court Order is ambiguous or appears to require disclosure of too much data it may be possible to query it with the Court, but the decision to do so needs to be made at an appropriate level of seniority.

2.2. Disclosures in the absence of a legal duty resulting in a choice to disclose or not. These may be in the 'public interest'/ to protect the public

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 a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual concerned and the broader public interest in the provision of a confidential service. The Police should always try and gain consent wherever possible. Valid consent removes any subsequent argument on the disclosure of information.

Some Acts of Parliament provide permission to disclose information but do not create a duty to do so. For example:

The Police and Criminal Evidence Act (1984) permits, but does not require, information to be disclosed to the Police if it is believed that someone may be seriously harmed or death may occur if they are not informed.

The Crime and Disorder Act (1998) permits disclosure to the Police if there is a need for strategic cross-organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in.

These are occasionally referenced by the Police when requesting information and so it is important to understand that, where there is a choice about whether or not to

disclose personal information to the Police, the requirements of both the Data Protection Act (1998) and the Common Law Duty of Confidentiality must be met. Staff should seek advice from the Caldicott Guardian, Information Governance Board (IGB) Lead or Information Governance (IG) Departmental staff in these circumstances.

In the absence of explicit consent, the Caldicott Guardian may authorise disclosure, the one-off Disclosure Log will be completed and held by the IG team , so that there is clear evidence of the reasoning used and the circumstances prevailing. The disclosure will also be added to the patient or staff record. The Lead Executive Director with responsibility for engagement with the Police must be informed.

Disclosures in the public interest should be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision making process and the advice sought is in the interest of both staff and the organisations they work within. Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. Where this is not forthcoming, the individual should be told of any decision to disclose against their wishes. This will not be possible in certain circumstances, e.g. where the likelihood of a violent response is significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation. This situation should be documented.

2.3. **Data Protection Requirements**

The Data Protection Act (1998) (DPA), which will be replaced in 2018 by new data protection legislation driven by the General Data Protection Regulation, sets out conditions that must be met when using or sharing information that identifies an individual, or could be used to identify an individual by matching it to other information. These include informing the individuals concerned about the sharing and use of information about them.

However, Section 29 of the DPA enables the work of the police to be exempt from a number of these requirements (though not all) where meeting them would undermine work to investigate and prosecute crime. Section 29 **does not** provide a duty to disclose information, nor does it override the requirements of the common law duty of confidentiality that must be met prior to disclosure being lawful (see below) – it does no more than relax the DPA requirements that need to be met.

The majority of formal requests by the Police for disclosure of personal information will be made under Section 29 of the DPA. This exempts Data Controllers (in this case the Health Board) from the normal, non-disclosure provisions.

Section 29 of the Act permits the disclosure of personal information without consent and allows information to be disclosed when required for:

- The prevention and detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax or duty or if any imposition of a similar nature.
- Where gaining consent would be likely to prejudice the investigation.

If consent is not possible or appropriate (e.g. the individual lacks capacity and cannot be given by a next of kin, or seeking consent will prejudice the Police inquiry), then Section 29 of the Data Protection Act is relevant. However, staff need to consider the Police request carefully when deciding (and create a proper audit trail) if there is an agreement to disclose without consent. It is for the Police to convince staff that disclosure should still be made without consent.

3. Procedures to Follow In the Release of Information

3.1 Making the Request

All requests from the Police for disclosure of personal information must be made **in writing**. Details must be provided on what grounds the information is being sought, i.e.

1. An official request without consent application form [sometimes referred to as F351 - see Appendix 1]. To be used when the individual has not given consent. This should contain details of what specifically is requested, as well as why the police want the information (Crime prevention, court order, time critical, public interest, prevent serious harm or death). It is through consideration of this information that the Health Board will decide whether or not to share the information. It must be signed by an Inspector or above.
2. If the request is for the specific provision of A&E medical notes, this utilises a different form (referred to as F185a or equivalent - see Appendix 2)
3. An official request with consent, this will contain details of what is requested and why the information is required. (see appendix 3 – this would also use F185a or equivalent)

3.2 Request for Health Records

During normal office hours (09:00–17:00), all requests for personal information about patients should be directed to the Health Records Department at the Princess of Wales Hospital (Subject Access Team).

Outside of these hours all urgent requests for personal information about patients should be directed to the senior on-call Manager for that site, contact details available via switchboard. The Lead Executive Director with responsibility for engagement with the Police must be informed.

The IG Department is available to give advice and support on all issues surrounding the sharing of patient or staff information during normal office hours (08:00–17:00).

In all cases the following must happen

- Immediately inform a member of the Senior Management Team or the on call manager if out of hours
- When the information relates to a significant investigation involving the Health Board the Lead Executive Director with responsibility for engagement with the Police must be informed.
- Obtain a receipt from the Officer removing the information;
- Complete an incident form on Datix (without naming the member of staff whose information has been shared) and if appropriate a Welsh Government ‘no surprises form’

- Inform IGB Lead within their governance support unit or department
- Completion of one off disclosure form and returned to IG department (Appendix 5). This should include a full record of what was given to the Police, together with a timeline of events leading up to the disclosure, this will include: Date & time of removal of records copies from Health Board premises; Name, rank & number of the Police Officer removing the copies of information.
- Update Health Record with details of disclosure

Only **copies** of medical or staff records should be given to the Police, Subject Access department will ensure the safe transfer of the information. The master copies must remain within the Health Board to ensure continuity of care for the patient. The exception to this is if the Police need to provide originals to the Coroner's Officer, where there isn't time for the records to be copied due to the seriousness of the investigation or where there is a need to forensically examine the physical notes to gather evidence (e.g. finger prints or DNA)

Whilst the property is retained by the Police it must be retained securely and confidentially. The Health Boards will require from the Police the safe return of all information, with proof of secure deletion of copies and an agreed process for the return of all property and equipment belonging to ABMU.

3.3 Requests for Staff Information and Records

All requests for personal information relating to staff should be directed to HR, the Head of Workforce Localities and Systems, during normal office hours (09:00–17:00), and copied to the Director of Workforce.

In all case the following must happen

- Immediately inform a member of the Senior Management Team or the on call manager if out of hours
- When the information relates to a significant investigation involving the Health Board the Lead Executive Director with responsibility for engagement with the Police must be informed.
- Obtain a receipt from the Officer if removing the information;
- Complete an incident form on Datix (without naming the member of staff whose information has been shared) and if appropriate a Welsh Government 'no surprises form'
- Inform IGB Lead within their governance support unit or department
- Completion of one off disclosure form and return to IG department (Appendix 5). Thisshould include a full record of what was given to the Police must be taken, together with a timeline of events leading up to the disclosure, this will include: Date & time of removal of records copies from Health Board premises; Name, rank & number of the Police Officer removing the copies of information;
- Update personnel file with details of disclosure

Whilst the property is retained by the Police it must be retained securely and confidentially. The Health Boards will require from the Police the safe return of all information, with proof of secure deletion of copies and an agreed process for the return of all property and equipment belonging to ABMU.

3.4 Provision of Emergency Department Medical Notes

A National Standard Operating Procedure (SOP) has been developed to provide guidance to all staff involved in the collection of medical evidence regarding the procedures to be followed when requests for A&E notes are made by the Police.

In such cases the Police Officer in charge of the case will contact the relevant Health Board employee, known as the NHS SPOC, to advise them that a medical request is en-route with the timescales for completion (i.e. 6 hours if suspect in custody, 48 hours if suspect known but not currently in custody). All requests should be accompanied by a correctly completed F185a (Medical Consent) form (Appendix 2).

On receipt of a correctly completed F185a form, the NHS SPOC will obtain the relevant A&E medical notes and scan them onto a secure area of the Health Board network before sending them to the police via the secure portal. See Appendix 2 for the process map of this procedure.

3.5 Requests for Equipment or Medical Devices

There may be instances where the Police request access to, or removal of, equipment, IT equipment, or medical devices as part of their investigations. This will invariably be to forensically examine the devices for evidence (e.g. physical evidence such as finger prints and DNA, or electronic evidence such as data files and audit logs). In these cases the Police will be covered by the Police & Criminal Evidence (PACE) Act 1984.

It is vitally important that an accurate record is taken of any IT equipment or medical device(s) handed over to the Police, including:

- Date & time of removal from Health Board premises
- Name, rank & number of the Police Officer removing the equipment
- Make & model of the equipment
- The serial number or asset number of the equipment
- Details of any patient, staff or organisational data known to be stored on the equipment.

In addition, staff handing over equipment should:

- Immediately inform a member of the Senior Management Team or the on call manager if out of hours
- When the information relates to a significant investigation involving the Health Board the Lead Executive Director with responsibility for engagement with the Police must be informed.
- Obtain a receipt from the Officer removing the equipment;
- Inform the IT Department (or EBME in the case of medical equipment) as soon as possible;
- Complete an incident form on Datix and if appropriate a Welsh Government ‘no surprises form’
- Inform the IG Department where it is believed that sensitive information or individual’s personal information (demographic or clinical) may be stored on the equipment; and
- Inform their IGB Lead within their governance support unit or department

- Complete the one-off Disclosure Log and return this to the IG Department (Appendix 5).

Whilst the property is retained by the Police it must be retained securely and confidentially. The Health Boards will require from the Police the safe return of all information, with proof of secure deletion of copies and an agreed process for the return of all property and equipment belonging to ABMU.

3.6 Reporting knife and gunshot wounds

It is generally accepted that the reporting of gun and knife wounds will be within the public interest; however, consent from the patient should be sought wherever possible. Professional regulatory guidance states that gunshot incidents should be reported to the Police; however, the patient's identity should not be disclosed without their consent.

A knife attack may be sufficient to justify a public interest disclosure of confidential information even where consent is not given, where it is likely to assist in the prevention and detection of a serious crime. Staff should consider the proportionality of any disclosures and always try to obtain consent where possible. Where this information is shared an incident form should be completed on Datix, the one-off Disclosure Log completed and returned to the IG Department, the patient record updated to reflect the disclosure and a Senior manager / IGB lead informed.

3.7 Road Traffic Accidents

Under road traffic legislation the Police may require the name and address of someone suspected of some forms of traffic offences (i.e. such as driving whilst under the influence of alcohol or drugs, causing a road traffic accident or failing to stop at the scene of an accident). The duty to disclose information to the Police is limited to information which may assist in the identification of the driver. It does not extend to disclosing details about the patient's injuries, or who else may have been with them. Where this information is shared an incident form should be completed on Datix, the one-off Disclosure Log completed and returned to the IG Department, the patient record updated to reflect the disclosure and a Senior manager / IGB lead informed.

.

3.8 Terrorism

Under terrorism legislation we are obliged to report suspected terrorist activity to the Police. Where this information is shared Where this information is shared an incident form should be completed on Datix, the one-off Disclosure Log completed and returned to the IG Department, the patient record updated to reflect the disclosure a and a Senior manager / IGB lead informed.

3.9 Missing Persons

If the Police enquire regarding a missing person, each case should be assessed to decide on the correct course of action regarding releasing information. The only possible grounds for disclosure are:

1. The patient's express consent is obtained to disclose the information to the Police (only applies to those patients who have capacity)

2. The disclosure is deemed to be in the patient's immediate best interests

3. The disclosure is in the public interest and is necessary and proportionate to prevent serious harm or death to the patient or another person

4. Where a Court orders that the disclosure takes place.

For example:

A. The Police would like to know if Mr Smith has attended A&E within the last 24 hours as he is an 82 year old who has dementia and has gone missing from a nursing home.

In these circumstances it would seem reasonable and in the patient's best interest to confirm if the patient has attended as they could be at risk of harm.

B. A young woman has not returned home after a night out and Police would like to know if she has attended as her family is concerned.

If the patient is an in-patient, consent must be sought if patient is conscious and has capacity. We must respect the individual's right to privacy, and in some cases they may not want to be found e.g. domestic abuse. If we confirm that the patient is on one of our wards without seeking consent, a family member they do not want to see may turn up and cause them harm and the Health Board would be at fault for breaching their confidentiality. This would not be the case if revealing the information was in the public interest or proportionate to prevent serious harm or death to the patient or another person.

C. A man who suffers with schizophrenia is missing and is known to be armed and dangerous by the Police, as he has already attacked a member of the public.

In this situation disclosure would be in the public interest as the man could cause harm to members of the public or to himself. However, for this type of request the Police could produce a request form (appendix 1) if a crime has been committed or can be prevented (see section 2.3).

In all cases, you must decide whether the breaching of the overall duty of confidentiality and trust between doctors and patients or any possible harm caused to the patient by disclosing this information, is outweighed by the benefits resulting from the disclosure. Generally speaking, this balancing exercise will only favour disclosure where the disclosure is necessary and proportionate (a) to prevent serious harm to the patient or others or (b) to assist in the detection/prevention of a crime.

Under 18's are classed as high risk, especially if they are known to have existing Safeguarding concerns. As such, information should be released to the police to assist them in locating the missing child/young person. If a child/young person discloses that they are missing in an attempt to flee the perpetrator of abuse, both the Police and Children's Social Care should be appropriately informed, to ensure the perpetrator is not inadvertently made aware of the child/young person's whereabouts.

3.10 Requests for Samples

A detailed departmental procedure for the management of the release of samples has been developed see appendix 4.

3.11 Patient's Evidence in Legal Proceedings

Where a patient, whether the individual is a suspect or a witness, is seriously ill, then due consideration and priority must be given to their clinical state and any hindrance to the recovery process. The decision to allow an interview with the police, solicitor or other concerned person is the ultimate responsibility of the Consultant-in-charge of the case.

The Consultant-in-charge in making this decision will have proper regard to the distress which the questioning may cause the patient who may or may not be beyond the hope of recovery.

All actions and information taken must be clearly documented in the Health Record which are timed, dated and signed with name printed. The Senior Nurse on duty will ensure a 'Clinical Incident' form is completed and will ensure that they obtain and record the full name and rank of the police officer/s concerned. They will ascertain the information and/or action required and why - in the Police's opinion - there is a need for this information.

☐

3.12 Safeguarding Information sharing

Where there is a disclosure of Violence Against Women, Domestic Abuse and Sexual Violence (VAWDASV), verbal consent will be obtained for referral to specialist services. The "Ask and Act" VAWDASV Pathway has been developed as a risk assessment tool and identifies the ongoing referral and information sharing process.

High risk victims of Domestic Abuse are informed that information will be shared with the appropriate Public Protection Unit for discussion at Multi Agency Risk Assessment Conference (MARAC). ABMUHB is a signatory of the South Wales Information Sharing Protocol. This process is fully explained in the ABMUHB Domestic Abuse Policy and Procedure (section 10) and also the ABMUHB Data Protection and Confidentiality Policy (section 11).

Information sharing where there are child protection concerns is clearly set out in Section 10.7 of ABMUHB Data Protection and Confidentiality Policy. Further information can be found in the Social Services and Well-being (Wales) Act 2014. Also ABMUHB Combined Safeguarding Children Guidance (includes links to Local and national Policies and Procedures) would be a useful resource.

MASH Health professionals working within a multi agency setting are guided by the same confidentiality Policy as those working in Health board settings, they may also be guided by a local multi-agency information sharing policy, along with this they make reference to The Wales Accord on the sharing of Personal Information (WASPI).

Child Practice Reviews - Protecting Children in Wales, Guidance for Arrangements for Multi-Agency Child Practice Reviews identifies a formal process to develop an anonymised child practice review report based on the merged timeline of significant events from the timelines of all agencies involved with the family including the police. Guidance is included where there are concurrent police investigations.

Multi Agency Adult Practice Reviews – the Social Services and Well-being (Wales) Act 2014 guidance (Vol. 3 – Adult Practice Reviews) indicates that the guidance for information-sharing outlined in CPS guidance for Child Practice Reviews, which provides a framework for the sharing of relevant information, would apply also to Adult Practice Reviews.

Procedural Response to Unexpected Death in Childhood (PRUDiC) - This procedure sets a minimum standard for a response to unexpected deaths in infancy and childhood and describes the process of communication and information sharing following the unexpected death of a child. It is a multi-agency procedural response intended to ensure consistency across Wales, and is not agency or discipline specific.

4. Further guidance

Please refer to the following for further advice on disclosure:

- The comprehensive Information Governance pages on ABMU's intranet site
- The NHS Wales Standard Operating Procedure for the Provision of A&E Medical Notes
- GMC – Confidentiality: reporting gunshot and knife wounds - https://www.gmc-uk.org/Confidentiality___Reporting_gunshot_and_knife_wounds.pdf_70063779.pdf
- Information Governance Alliance – Disclosure of Information to the Police - https://www.igt.hscic.gov.uk/Resources/Disclosure%20of%20Personal%20Information%20to%20the%20Police.pdf
- Information Commissioners Office – Using the Crime and Taxation exemptions of the Data Protection Act. https://ico.org.uk/media/for-organisations/documents/1594/section-29.pdf

Appendix 1 – Police Form Under Section 29, no consent - **(Police originated form copy below is an example)**

RESTRICTED WHEN COMPLETE

Personal Data Request Form

To .....

Organisation & Address.....

This request for personal data and other information is made under the powers invested in me as a Constable of the South Wales Police by the Police Act 1996 (section 30(1) which gives Constables all the powers and privileges of a Constable throughout England and Wales and Section 30(5) defines powers as powers under any enactment whenever passed or made). These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order.

The personal data I require relates to the following individual(s):

I require the following personal data and **other information:**

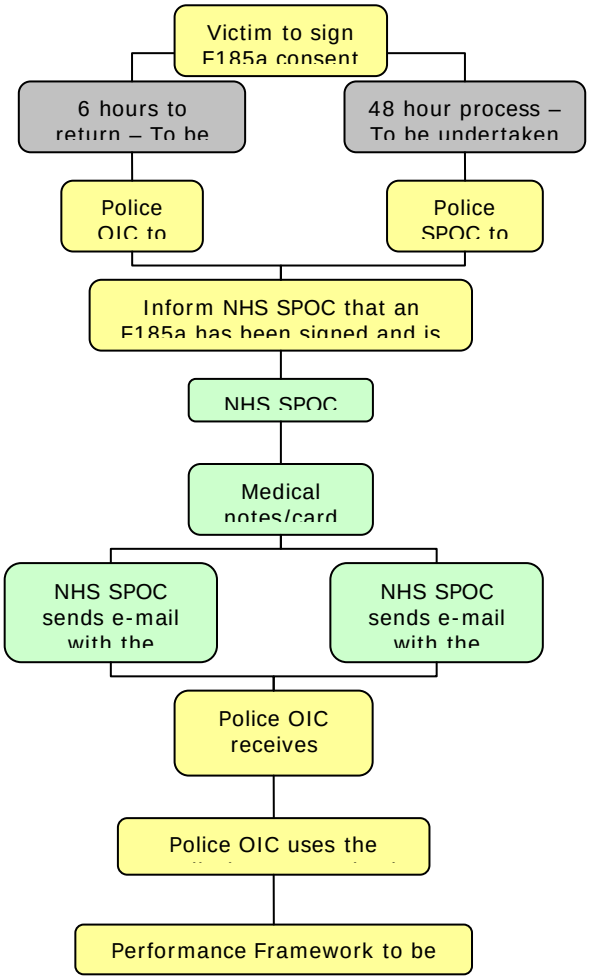
I require the personal data and **other information** to assist with my enquiries into:

I confirm that the personal data and other information is required for the following purpose(s):

tick	Purpose	Legal Basis
	For the prevention, investigation and detection of crime	Police Acts, Common law
	For the apprehension and prosecution of offenders	Police Acts, Common law
	To protect life or property	Police Acts, Common law
	To confirm or corroborate information for intelligence purposes	Police Acts, Common law
	To put before a court to obtain a search warrant	Police Acts, Common law
	To prepare a file for the Coroner's court	On request of the Coroner
	To further a money laundering or confiscation investigation	Proceeds of Crime Act 2002

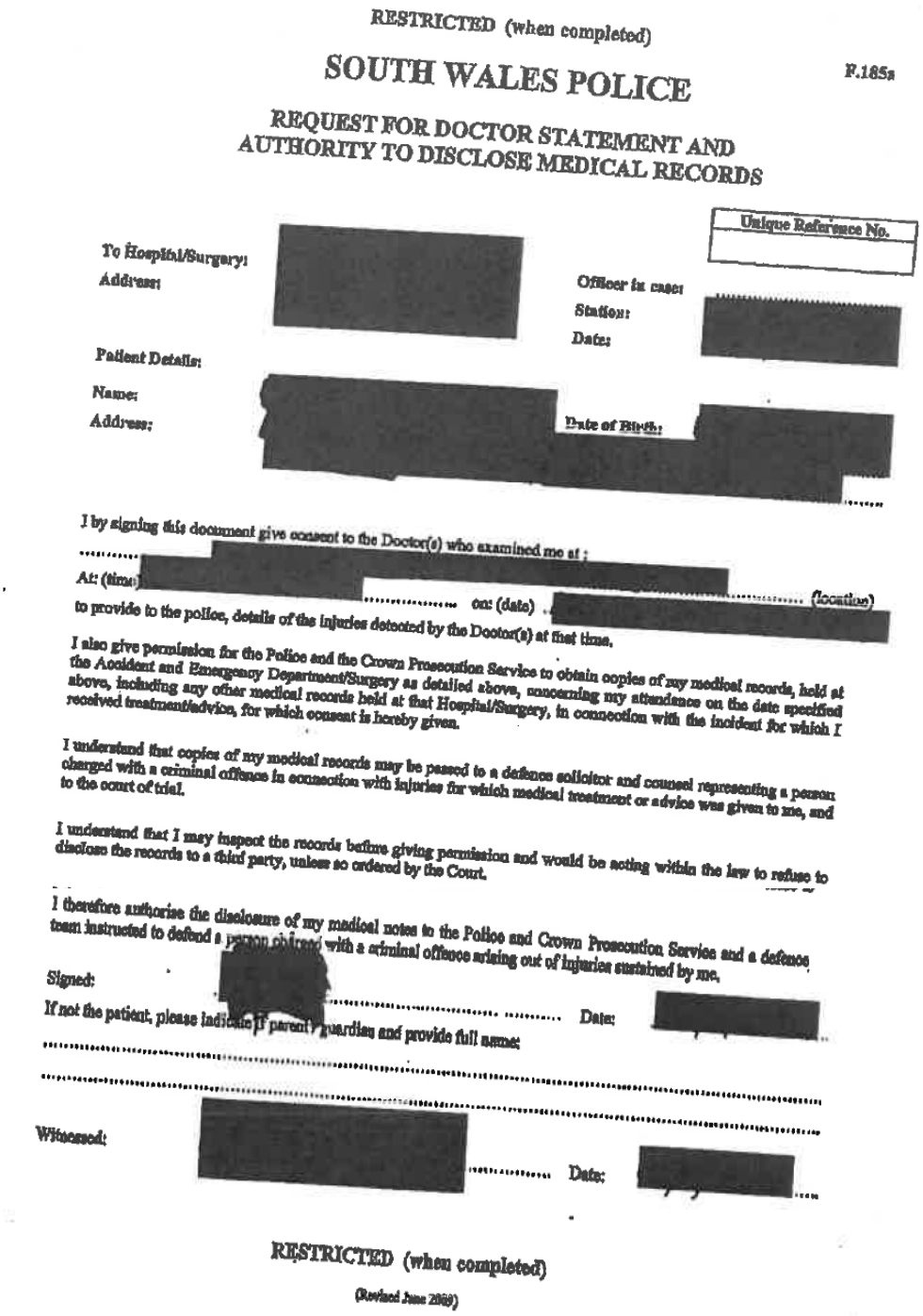
RESTRICTED WHEN COMPLETE- NEED TO KNOW BASIS ONLY
COPY TO BE KEPT WITH INVESTIGATION PAPERS
1 of 4

Appendix 2 – Process map for provision of A&E Medical Notes



Appendix 2 – Application of provision of A&E Medical Notes (Police originated form copy below is an example)

Put in copy of F185



RESTRICTED (when completed)

SOUTH WALES POLICE

F.185a

REQUEST FOR DOCTOR STATEMENT AND AUTHORITY TO DISCLOSE MEDICAL RECORDS

Unique Reference No.

To Hospital/Surgery:
Address:

Officer in case:
Station:
Date:

Patient Details:
Name:
Address:

Date of Birth:

I by signing this document give consent to the Doctor(s) who examined me at :

At: (time) ..... on: (date) ..... (location)

to provide to the police, details of the injuries detected by the Doctor(s) at that time.

I also give permission for the Police and the Crown Prosecution Service to obtain copies of my medical records, held at the Accident and Emergency Department/Surgery as detailed above, concerning my attendance on the date specified above, including any other medical records held at that Hospital/Surgery, in connection with the incident for which I received treatment/advice, for which consent is hereby given.

I understand that copies of my medical records may be passed to a defence solicitor and counsel representing a person charged with a criminal offence in connection with injuries for which medical treatment or advice was given to me, and to the court of trial.

I understand that I may inspect the records before giving permission and would be acting within the law to refuse to disclose the records to a third party, unless so ordered by the Court.

I therefore authorise the disclosure of my medical notes to the Police and Crown Prosecution Service and a defence team instructed to defend a person charged with a criminal offence arising out of injuries sustained by me.

Signed: ..... Date:

If not the patient, please indicate if parent / guardian and provide full name:

.....

.....

Witnessed: ..... Date:

RESTRICTED (when completed)

(Revised June 2009)

Appendix 3 – Release of Information with Consent - F185a

~Release of Information without consent – F351

RESTRICTED WHEN COMPLETE

F351
For

Personal Data Request Form

To *(name and position known)*..... .....

Organisation & Address.....

.....

This request for personal data and other information is made under the powers invested in me as a Constable of the South Wales Police by the Police Act 1996 (section 30(1) which gives Constables all the powers and privileges of a Constable throughout England and Wales and Section 30(5) defines powers as powers under any enactment whenever passed or made). These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order.

The personal data I require relates to the following individual(s):
(Include identifying details of the person where known, such as name, address and date of birth)

I have the following information to assist you in locating the personal data and other information:
(Include further details, where available, to assist locating the information sought)

I require the following personal data and other information:
(Describe the information sought)

The following details and documents are required,

I require the personal data and other information to assist with my enquiries into:
(Describe the subject of those enquiries as far as possible without prejudicing them)

I confirm that the personal data and other information is required for the following purpose(s):

RESTRICTED WHEN COMPLETE- NEED TO KNOW BASIS ONLY
COPY TO BE KEPT WITH INVESTIGATION PAPERS
1 of 5

Tick the relevant box(es) and complete the "other" row where necessary

tick	Purpose	Legal Basis
	For the prevention, investigation and detection of crime	Police Acts, Common law
	For the apprehension and prosecution of offenders	Police Acts, Common law
	To protect life or property	Police Acts, Common law
	To confirm or corroborate information for intelligence purposes	Police Acts, Common law
	To put before a court to obtain a search warrant	Police Acts, Common law
	To prepare a file for the Coroner's court	On request of the Coroner
	To further a money laundering or confiscation investigation	Proceeds of Crime Act 2002
	To risk assess the address to safeguard the health and safety of any emergency personnel attending	Police Acts, Health & Safety, Common law
	To identify if there are children at the address to negate any harm caused by police action	Children Act 2004
	To locate a missing person to ascertain their well being	Police Acts, Common law
	To progress enquiries into a Road Traffic Incident	Police Acts, Common law
	Other (please specify)	

I request that the personal data and other information should be provided to the Police in the following manner:-
(Having considered factors such as the protective marking indicate how the information should be provided to the
Police, e.g. in person, by post, by secure email etc)

The information will be regarded as confidential and as such will be collected by Officers in person.

The Data Protection Act 1998 defines personal data as data which is biographical in nature, has the applicant as its focus and/or affects the data subject's privacy in his or her personal, professional or business life. Under the Data Protection Act 1998,

disclosure of personal data:-

- For the prevention and detection of crime or the apprehension or prosecution of offenders is permitted under s29 (3);
- Required by or under any enactment, by any rule of law or by order of the court is permitted under s 35 (1) (including the Health and Safety Act);
- For the purpose of, or in connection with, any legal proceedings is permitted by s35 (2) (a);

Where no data protection exemption applies, consideration should be given to the first principle issue of fairness. Where the rights and freedoms or the welfare of an individual is in doubt, a harm test should be applied. It is highly unlikely disclosure would be unfair in these circumstances.

Human Rights Act 1998 Article 8 – right to privacy. This request is consistent with Article 8(2) prevention of disorder or crime.

To be completed by the officer requesting the personal data and other information – tick appropriate box(es)

I confirm that: -

☐ this information will be used in connection with this enquiry and held and used only as long as this is required for policing purposes and any subsequent criminal justice proceedings;

☐ if this personal data is not disclosed it will prejudice the prevention or detection of crime or the apprehension or prosecution of offenders;

☐ if this personal data is not disclosed it will prejudice the purpose ticked above;

Signed……Collar No……Date……..

Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to **police staff.**

Signed……Force No……Date……..

Print Name……Post……..

BCU/Area/Dept Address……..……..

Phone……Fax……..Email……..……..

RESTRICTED WHEN COMPLETE- NEED TO KNOW BASIS ONLY
COPY TO BE KEPT WITH INVESTIGATION PAPERS
3 of 5

RESTRICTED WHEN COMPLETE

If the nature of the enquiries is specified above, this form must be countersigned by an an Officer of at least the rank of Inspector or Supervisor. If the investigation is such that no explanation can be given, this form will be countersigned by a Superintendent.

Countersigned .....Collar No.....Date.....

Print Name.....Post.....

This section to be completed by the recipient of the request for personal data and information.

Response

Please reply to all requests so that we know it has been considered and to help prevent duplication.

As part of your decision making process, please take into account the requirements upon your organisation/you in relation to the request, for example the Crime and Disorder Act 1998, (any person or organisation has a power to provide information to a relevant authority in order to achieve a crime and disorder objective), the Local Government Act, Children Acts 1989 and 2004, and other legislation relevant to your organisation.

Signature.....Date.....

Name.....Position.....

Organisation & Dept.....

Delete one of the following options as applicable:

- The information requested above has been approved for disclosure and is attached;
- The information requested above has not been approved for disclosure;

Please explain why you have decided not to disclose the information so that we know whether you need additional information, or for us to consider presenting to the Court to obtain a Disclosure Order

RESTRICTED WHEN COMPLETE- NEED TO KNOW BASIS ONLY
COPY TO BE KEPT WITH INVESTIGATION PAPERS
4 of 5

.....

.....

.....

.....

If there is insufficient room please continue on an additional sheet.

The subject of this request should not be given any indication that this request has been made prior to consultation with the requesting Officer. If your organisation subsequently receives a request for a copy of this document (e.g. under the Data Protection Act 1998 or the Freedom of Information Act 2000) for this information, please contact the requesting Officer.

Appendix 4

SOP Releasing Samples for Police or Specialist Nurses in Organ Donation

1. Introduction

All telephone calls from the Police regarding release of samples and/or results must be referred to one of the Consultant Staff.
All telephone calls from a Specialist Nurse in Organ Donation regarding release of samples should be handled directly by the relevant qualified Biomedical Scientist.

This Procedure refers to biological material submitted to the laboratory as part of the clinical investigation of a patient under the care of a consultant medical practitioner. Although reference is made throughout to biological materials and/or samples, this policy should be deemed to include any information relating to that sample. For example, work-sheets, quality control records, vertical audit data and results obtained from examination of the sample.

The laboratory has a duty of care to the patient and not the Police, but the Data Protection Act and other supporting legislation does enable the sharing of patient information in the wider public interest.

Occasionally the Police request that samples taken from patients for clinical reasons are given to them for forensic analysis. If the Police express interest in a sample then it must not be disposed of. The matter should be brought to the attention of the Head or Deputy Head of Department immediately. The sample must then be stored safely until it is decided whether the sample may be released. Under no circumstances should any material be given to the Police by anyone other than the Head or Deputy Head of Department.

Release of samples without following the correct procedures may lead to the prosecution of the Health Board (HB).

2. Scope and Purpose

Target user groups and their depth of knowledge of the policy are:

- Consultant Staff must have full knowledge and understanding
- Clinical Scientists, Section Managers and all Biomedical Scientist Groups must have a working knowledge
- Laboratory Support Workers must be aware of the policy

3. Responsibilities – Ownership of samples

The laboratory acts as the custodian of samples and does not own them. The patient gives implied consent for tests to be performed upon any sample collected from them for clinical reasons. In the absence of specific instructions regarding the disposal of the samples, implied consent is also taken that such samples may be disposed of by routine means, when work is finished. Specific consent from the patient is needed for any other purpose in cases where the patient is competent to give that consent. If the Police receive consent to release a sample then ownership of the sample is with the Police, and subsequent disposal of a sample could be interpreted as tampering with evidence (as it is under ownership)

4. References – Legal Framework

Data Protection Act 1998:

Under the Data Protection Act, there are provisions made to release information to other organisations without patient consent.

A request from the Police under Section 35 relates to information needed for a court case and this is usually accompanied by patient consent. If not, then the Information Governance Manager must be contacted on 01792 703293.

A request from the Police under Section 29 relates to information needed for a criminal investigation and usually does not come with patient consent. The Police must complete a Section 29 form, signed by an Inspector or above, and this must be approved by the Information Governance Manager or, in his/her absence, the Caldicott Guardian, before release of the information.

Legally, the HB only ever has to release information to the Police on receipt of a Court or Judge's Order. A Section 35 or Section 29 request can be considered by the HB and refused on reasonable grounds.

The Police and Criminal Evidence Act 1984

The Police and Criminal Evidence Act 1984 defines materials that the police can take in evidence. Human tissue or material that have been collected for the purposes of diagnosis or medical treatment are specifically ***excluded*** in Section 11 of this Act. This means that such samples cannot be released until the correct procedures are followed. Section 29 of the Data Protection Act may be used to gain access to such samples.

5. Definitions

'Not Applicable'

6. Related Documents

LMS-A-SOP Saving Samples for Police
LMS-A-FORM Release of Samples to Specialist Nurses in Organ Donation
LMS-A-FORM Release of Sample to Police

7. Procedure

7.1 Safeguarding Samples

Usually, a police officer will approach the laboratory by either telephoning or calling in person. If the Head or Deputy Head of Department are available they should be contacted. Otherwise, the name, serial number and work address of the officer making the approach should be recorded as well as the details of the sample(s) being sought.

For more information, see Document: [LMS-A-SOP Saving Samples for Police].

7.2 Patient Confidentiality

Results of investigations performed by the laboratory are considered to be sensitive personal data under the Data Protection Act 1998. The inappropriate release of results would be a breach of this Act. Results may only be disclosed with the written consent of the patient. The only exception to this is for the purpose of preventing or detecting a crime, or the apprehension or prosecution of offenders. This should be discussed with the medical Consultant caring for the patient and the Information Governance Manager or Caldicott Guardian. The Police may obtain a Court or Judge's Order or a Section 29 Data Protection Act request to view the patient's records.

7.3 Approaches by Specialist Nurses in Organ Donation

Occasionally, and sometimes during the out-of-hours periods, laboratory staff will be contacted by telephone by a Specialist Nurse in Organ Donation, requesting the release of stored blood samples taken from as close a time as possible to the time of the patient's admission to hospital. The Specialist Nurse will always identify themselves on the telephone by their designation and name. The requested samples are from an individual who has gone on to become an organ donor, and samples will be collected by the named Specialist Nurse from the laboratory as soon as possible after the telephone call has been made and the samples have been retrieved. The samples will be entered into a national donor specimen biobank and database, the aim of which is to improve the quality of organ donation. Appropriate approvals have been granted by ABMU Health Board, and as such, these samples can be released directly to the Specialist Nurse. The appropriate "release of specimens" form will need to be completed at the time of sample handover [LMS-A--FORM Release of Samples to Specialist Nurses in Organ Donation], and then given to the Departmental Secretaries for filing.

7.4. Request for a sample when the patient is alive

If a patient is alive and conscious then he or she must first give written consent that any sample may be given to the Police. The laboratory must receive this consent prior to the release of the sample. The only exception to this is if an approved Section 29 Data Protection Act request has been received.

There may be times when there is insufficient blood to both perform outstanding medical tests and to release a sample to the Police. Under these circumstances the decision rests with the consultant medical practitioner caring for the patient as to what should be given priority, acting in the patient's best interests.

If the patient is unconscious, but expected to recover, any samples requested should be recovered and stored under suitable conditions to maintain sample integrity until such time as the issue of consent is resolved (as per Section 4 of this Policy).

If the patient is unconscious and not recovering, then the consultant medical practitioner caring for the patient takes responsibility in the first instance for any samples and must act in the best interests of the patient. A Section 29 Data Protection Act form is needed from the Police.

The consultant medical practitioner caring for the patient may think it appropriate that the views of the next of kin are obtained. However, it should be made clear that the *next of kin have no authority to act on behalf of the patient.*

If permission is not obtained, the police cannot demand that the laboratory release a sample against the patient's wishes or the wishes of the consultant medical practitioner caring for the patient. They must obtain a Court Order from a Circuit Judge (not a magistrate) (this is for sample release but not for release of results, when a Section 29 Data Protection Act request is required) in order to over rule the wishes of the patient in compliance with the Police and Criminal Evidence Act 1984, Section 9. Before making an application to a Judge, the Police must serve notice on the HB advising them of the date and time of the court hearing. If any of the above conditions are met, subsequent disposal of the sample could be interpreted as tampering with evidence.

7.5 Request for a sample when the patient is dead

Once deceased, the patient has no rights under the Data Protection Act. The Coroner investigating the death, or one of his officers, may request one or more of the patient's samples. These should always be released (through the Head or Deputy Head of Department) and a sample release form completed [LMS-A-FORM Release of Samples to Police].

If the death is being investigated by anyone other than the Coroner then advice should be sought from the Information Governance Manager or Caldicott Guardian as to the advisability of releasing the sample. The relatives of the deceased person may have some say in what happens to a sample under these circumstances.

8. Safety Information/Risk Assessments

Samples must be stored in such a way as to minimise risk of infection or other hazard to any member of staff.

Samples must be packaged for release in such a way as to minimise risk of infection or other hazard to the receiving Police Officer.

The Police Officer must sign a receipt form confirming that the sample is labelled in such a way as to adequately identify the patient and that the sample is released on the understanding that it has not been subject to a formal "chain of custody" procedure.

Appendix 5 – One off disclosure form

Please fill in your entries below and return to Jessica Hiscock in the IG Department via email :

Hospital No	Patient Name and DOB	What is being shared?	Why?	Who with?	When?	Consent status	Date when patient notes updated to detail this disclosure*

* Must always be done asap

Examples

Z1234567	Becky Wadley 08.12.70	1. Clinical details of admission 01.08.17-10.08.17 2. Demographic data	For continued support	Mary Smith, support worker, at the RNIB in Cardiff	12.09.17	Explicit consent to share received from patient 08.09.17	12.09.17
Z9876543	John Morgan 15.05.92	ED records from attendance on 07.09.17	Section 29[i] request received	South Wales Police, PC David Harvey, badge number 66883	13.09.17	No consent sought due to section 29 request	13.09.17

[i] Section 29 allows ABMU to share information with the police, if we wish to, without asking for consent because by asking for that consent, it may prejudice the police's criminal investigation