GIG CYMRU NHS WALES — Bwrdd Iechyd Prifysgol Caerdydd a'r Fro Cardiff and Vale University Health Board	**Reference Number: UHB 290** **Version Number: 1** **Date of Next Review:22 Jun 2018** **Previous Trust/LHB Ref Number: N/A**

Personal Information
Use and Disclosure of and the Duty to Share
Guidance

Introduction and Aim

There are legal restrictions on how personal information may be used stemming from the Data Protection Act 1998, and where personal information is held in confidence (e.g. to provide care and treatment), the common law places additional constraints on its disclosure. Usually a form of consent is required, unless the disclosure is required by Court Order or under an Act of Parliament. Staff must be made aware of the right of an individual to restrict how confidential personal information is disclosed and the processes that they need to follow to ensure this right is respected.

Staff making decisions about sharing health and social care information cannot rely only on compassion and common sense. They must also act within the law. Every minute of every day, staff employed across the health and social care system make lawful use of personal confidential data about patients and service users. All uses of such data are known as 'processing', including holding, obtaining, recording, using and sharing.

The Data Protection Act 1998 provides conditions that must be satisfied prior to using or disclosing (both termed processing in the Act) personal information. Where personal information is held in confidence (e.g. health records or case file information) common law obligations additionally require the consent of the subject of the information before it is disclosed to a third party unless exceptional circumstances apply.

This document provides guidance to be followed by Cardiff and Vale University Health Board (the UHB) to ensure that we adhere to the appropriate legislation and will have a consistent approach for sharing personal information in all settings. This guidance supports the UHB's overarching Information Governance Policy and Information Governance Control Document Framework and satisfies the requirements of Welsh Government.

The guidance will ensure that all staff understand the requirements placed upon them in respect of sharing personal information and personal sensitive information thereby mitigating any potential risks resulting from non compliance with legislation such as substantial fines or enforcement notices from the Information Commissioner. In addition this guidance will ensure that all UHB staff will understand when sharing information for the direct provision of care can take place correctly, and as a consequence will directly impact on patient care and outcomes.

Objectives

- Set out agreed guidance for staff on sharing personal information.
- Provide sufficient guidance to empower staff when making difficult decisions on when it is appropriate to share or not to share in differing situations.
- Provide guidance on consent issues.
- Provide definitive guidance for staff on standards and good practice when sharing personal information for care purposes.
- Provide guidance for staff on the recognised professional standards of good practice.
- Assist staff to differentiate between sharing personal information for care purposes and non care purposes.
- Ensure that all staff understand the requirements placed on them when sharing personal information.
- Ensure that the UHB reduces any risk associated with incorrect or inappropriate sharing of personal information.

Scope

This procedure applies to all of our staff in all locations including those with honorary contracts.

Equality Impact Assessment	An Equality Impact Assessment has not been completed as this procedure has been written to support the Information Governance Policy. The Equality Impact Assessment completed for the Policy found there to be some impact in relation to communication and an Action Plan has been developed to address the issues.
Documents to read alongside this Procedure	Information Governance Policy Data Protection Act 1998 Equality Act 2010 Data Protection Policy Disclosure of Personal Data to the Police Guidelines GMC Guidance on Confidentiality NMC Code for Nurses and Midwives NICE Clinical Guideline 138 –Patient Experience in Adult NHS Services
Approved by	Information Governance Sub Committee
Accountable Executive or Clinical Board Director	Medical Director – Caldicott Guardian Board Secretary – Senior Information Risk Officer (SIRO)
Author(s)	Corporate Governance Senior Information and Communication Manager

Disclaimer

If the review date of this document has passed please ensure that the version you a using is the most up to date either by contacting the document author or the [Governance Directorate.](#)

Summary of reviews/amendments			
Version Number	**Date of Review Approved**	**Date Published**	**Summary of Amendments**
1	22/06/2015	06/04/2016	New Document

Contents Page

Use and Disclosure of and the Duty to Share Personal Information Guidance

1 Legal Requirements

1.1 Data Protection Act 1998 Conditions

The Data Protection Act 1998 provides eight **Principles** that apply to all use and disclosure of personal information.

Personal data must be:

1 Processed Fairly and Lawfully
2 Processed for specified purposes
3 Adequate, Relevant and not Excessive
4 Accurate and kept up to date
5 Kept for as long as is necessary and no longer
6 Processed in line with data subjects rights
7 Processed securely
8 Only transferred to other countries that have suitable data protection controls

In addition to satisfying these eight Principles, organisations must also satisfy one condition from a supplementary schedule (2) and where the information is deemed sensitive under the provisions of the Act a further condition from a second supplementary schedule(3). It is important to note that where a care organisation is using and disclosing personal information for purposes relating to the care of an individual the Data Protection Act will not prevent that use or disclosure. However, other uses or disclosures are likely to require the explicit consent of the individual concerned.

1.2 Common Law Obligations

The Common Law requires that there is a lawful basis for the disclosure of personal information that is held in confidence. Unlike the Data Protection Act which applies to legal organisations in their entirety, the common law applies to the clinic, team or workgroup caring for an individual, ie those not caring for the individual cannot assume they can access confidential information about the individual in a form that identifies them. Normally the basis of access will be consent which must be sought before disclosure of the information. It is generally accepted that this consent can be implied where the purpose is directly concerned with an individual's care or with the quality assurance of that care and the disclosure should not reasonably surprise the person concerned. NB: Consent **cannot** be implied when an individual has expressly dissented.

In other circumstances and for other purposes, consent cannot be implied and so must be specifically sought or there must be some other lawful basis for disclosing the information.

1.3 Caldicott Principles

Caldicott Principles 1997 (includes a new seventh Caldicott Principle in 2013)

1. Justify the purpose(s):
2. Don’t use personal confidential data unless it is absolutely necessary:
3. Use the minimum necessary personal confidential data:
4. Access to personal confidential data should be on a strict need-to-know basis:
5. Everyone with access to personal confidential data should be aware of their responsibilities:
6. Comply with the law:
7. The duty to share information can be as important as the duty to protect patient confidentiality: **(New Principle)**

Information Governance review March 2013 Link here

2 Consent

Most people who use health and social care services accept and expect that doctors, nurses and other professionals will need to share personal confidential data if they are going to provide optimum care.
People get frustrated if they have to answer the same questions repeatedly as they move along a care pathway. It may be good professional practice for a clinician to check an item in a medical record by asking the patient to expand on a previous answer. However, it is not good practice for important information to be missing from the record. Patients and service users want the professionals to act responsibly as a team.

There is in effect an unwritten agreement between the individual and the professionals who provide the care that allows this sharing to take place.

This requires the health and social care professional to treat the patient on the basis of their needs and keep the patient’s information confidential. In return, the health and social care professional is able to rely on ‘implied consent’ when sharing personal confidential data in the interests of direct care, as long as the patient does not object, or has not already done so.

Patients therefore trust professionals to both protect their personal confidential data, and share information safely in the interests of their care and imply they consent to their information being shared in these settings.
18 GMC guidance on confidentiality, http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_24_35_disclosing
NMC Code for Nurses and Midwives

2.1 Definitions of consent

Consent is the approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be ‘no surprises’) and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.

2.2 Explicit consent

Explicit consent is unmistakeable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. It must be noted that a patient may have capacity to give consent, but may not be able to write or speak and staff need to record such situations in the record. In circumstances where patients lack capacity further information is provided in section 6.3 below. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual’s direct health and social care.

2.3 Implied consent

Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of the use of implied consent include doctors and nurses sharing personal confidential data during handovers without asking for the patient’s consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation on the basis of implied consent

- Safe and appropriate sharing in the interests of the individual’s direct care should be the rule, and not the exception.
- However, the need to share some information does not entail the sharing of everything.
- Only relevant information about a patient should be shared between professionals in support of their care.

3 Sharing Personal Information for Care Purposes

3.1 It should be noted that this guidance does not affect the duty to share information for care purposes. This duty was re-asserted by the

Caldicott 2 Review Panel in their report 'Information - To share or not to share: The Information Governance Review'.

3.2 Caldicott Principle 7 states **that "the duty to share information can be as important as the duty to protect patient confidentiality".** This means that health and social care professionals should have the confidence to share information in the best interests of their patients/service users within the framework set out by the Caldicott Principles. They should be supported by the policies of their employers, regulators and professional bodies.'

3.3 This new principle seven has been further supported by the Welsh Government and the expectation is that relevant personal confidential data **should be shared** among 'registered and regulated health and social care professionals who have a legitimate relationship with the individual' and even supports sharing of information with other members of the care team such as allied health professionals and therapists if there are 'appropriate safeguards' in place.

3.4 For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual. Health and social care providers should audit their services against NICE Clinical Guideline 138, specifically against those quality statements concerned with sharing information for direct care.

There should be a presumption in favour of sharing for an individual's direct care and that the exceptions should be thoroughly explained, not vice versa. The motto for better care services should be: 'To care appropriately, you must share appropriately'. Examples of organisations can be found in section 8.

3.5 In the past, information governance rules have prioritised systems over people. Too often they have been seen as an insurmountable obstacle and an excuse to avoid sharing information. The new principles outline a new approach. This new approach will mean that frontline staff will be confident about when to share information with other members of a person's care team and how to do so safely.

4 Professional standards and good practice when sharing information for care purposes

All processing of such data must be lawful. There are four legal bases for processing personal confidential data which meet the common law duty of confidentiality. These are:

- with the **consent** of the individual concerned.;

- through **statute**, such as the powers to collect confidential data in section 251 of the NHS Act 2006 (see section 6.7) and the powers given to the Information Centre in the Health and Social Care Act 2012 (see sections 1.8, 6.5 and 7.3.4);
- through a **court order**, where a judge has ordered that specific and relevant information should be disclosed and to whom;
- when the processing can be shown to meet the ‘**public interest test’**, meaning the benefit to the public of processing the information outweighs the public good of maintaining trust in the confidentiality of services and the rights to privacy for the individual concerned.

4.1 In addition to having one of these legal bases, the processing must also meet the requirements of the Data Protection Act and pass the additional tests in the Human Rights Act. Any processing of personal confidential data that is not compliant with these laws, even if otherwise compliant with the Data Protection Act, is a data breach, and must be dealt with as such.

4.2 In some cases of direct care, the transfer of necessary and relevant information between organisations can be poor. This can cause frustration and distress for patients, and potentially affect the quality of care received.

4.3 Health and social care professionals and staff may sometimes be asked for sensitive information about a patient, for example, when an individual calls an organisation seeking information about a patient they claim is a relative. Staff must ensure that the patient is happy for their information to be shared with the person making the call.
Care must be taken to ensure any caller is legitimate, and that it is appropriate for personal confidential information to be shared with them.

4.4 Staff should check that any callers, by telephone or in person, are who they say they are. **There can be a significant risk of harm to a patient through impersonation by those seeking information improperly**. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information. Inevitably, there are occasions when professionals and staff disclose personal confidential information by mistake. Such mistakes can result in serious consequences. Staff should report such instances using incident reporting process.

All staff have a duty to protect the confidentiality of personal information that is held by them and in the organisation.

You should aim:

- to inform patients about the use of their confidential data and to record their objections, consent or dissent;
- to provide access to a patient's data to other relevant professionals, always doing so securely, and only where there is a legal and appropriate basis to do so
- to share information with legitimate relatives, carers and next of kin if patient is happy for information to be shared.

5 Personal confidential information/data

This is data in which individuals are clearly identified, or are easily identifiable. This data should not be processed without a clear legal basis.
Personal confidential data should only be disclosed with consent or under statute and any disclosure must always be limited and accompanied by a contractual agreement that mitigates the risk of misuse and inappropriate disclosure. The contractual agreement needs to set out, as a minimum, the legal basis for the data flow, the purposes to which the data can be put, the safeguards that should be in place to protect data and how the public are informed about these.

6 Using the Information for Purposes not directly linked to Care Services

Where an organisation wishes to disclose confidential personal information for a purpose not directly related to care, consent cannot be implied. In most cases, individuals should be asked for their explicit consent for information to be shared with non-care organisations, for example:

- housing departments;
- education services;
- voluntary services;
- Sure Start teams;
- the police;
- government departments.
- local authorities

Individuals must also be asked for explicit consent for their confidential personal information to be shared for non-care purposes, such as those detailed below

Non-care purposes

a) Checking quality of care

- Testing the safety and effectiveness of new treatments and comparing the cost-effectiveness and quality of treatments in use;
- Care audit activity on site with external agencies such as HIW
- Supporting audit studies;
- Comparative performance analysis across clinical networks;
- Ensuring the needs of service users within special groups are being met eg children at risk, chronically sick, frail and elderly.

b) Protecting the health of the general public

- Drug surveillance (pharmacovigilance) and other research-based evidence to support the regulatory functions of the Medicines and Healthcare products Regulatory Agency;
- Surveillance of disease and exposures to environmental hazards or infections and immediate response to detected threats or events;
- Vaccine safety reviews;
- Safety monitoring of devices used in healthcare;
- Linking with existing National Registries for diseases / conditions;
- Analysis of outcomes following certain health interventions (ie public health interventions as well as treatments);
- Monitoring the incidence of ill health and identifying associated risk factors; and
- Identifying groups of patients most at risk of a condition that could benefit from targeted treatment or other intervention.

c) Managing care services

- Capacity and demand planning;
- Commissioning;
- Data for Standards and Performance Monitoring;
- National Service Frameworks;
- Clinical indicators;
- Information to support the work of the Care Quality Commission;
- Evidence to support the work of the National Institute for Health and Clinical Excellence;
- Measuring and monitoring waiting times, in support of the waiting times targets;
- Data to support Productivity Initiatives;
- Agenda for Change;
- Benchmarking.

d) Supporting research

- Assessing the feasibility of specific clinical trials designed to test the safety and/or effectiveness and/or cost-effectiveness of healthcare interventions;
- Identification of potential participants in specific clinical trials, to seek their consent;
- Providing data from routine care for analysis according to epidemiological principles, to identify trends and unusual patterns indicative of more detailed research;
- Providing specific datasets for defined approved research projects.

6.1 Public Interest justification

Where explicit consent cannot be obtained the organisation may be able to rely on the public interest justification or defence. This is where the organisation believes that the reasons for disclosure are so important that they override the obligation of confidentiality (eg to prevent someone from being seriously harmed).

6.2 Court Order or Act of Parliament

Disclosure may also be required by Court Order or under an Act of Parliament, i.e. there is a statutory or other legal basis for the disclosure. Of particular note in this respect are disclosures permitted under section 251 of the NHS Act 2006, formerly known as section 60 of the Health and Social Care Act 2001. Applications for approval to use Section 251 powers are considered by the Confidentiality Advisory Group (CAG) of the Health Research Authority.

The advice of specialist staff, eg Caldicott Guardians or legal advisors should be sought prior to making disclosures in the public interest or where a Court Order or statutory basis is provided as justification.

6.3 Best Interests decisions

In general no-one may consent on behalf of another individual who has the capacity and competence to decide for themselves. However, treating clinicians, parents of young children, legal guardians, or people with powers under mental health law, e.g. the Mental Capacity Act 2005 must make decisions that they believe are in the best interests of the person concerned.

It should also be borne in mind that an individual has the right to change their mind about a disclosure decision at any time before the disclosure is made, and can do so afterwards to prevent further disclosures where an activity requires a regular transfer of personal information. In addition, individuals do not have to agree to a professional sharing information about them with their carer, family or friends. If individuals tell a professional that they do not want anyone to be given information about them this must be respected and acted upon.

7 Staff Guidelines on Respecting Disclosure Decisions

To ensure individuals’ rights to restrict disclosure of their personal information are respected, staff should be made aware of these rights and be provided with information leaflets and the organisation’s confidentiality code of conduct or equivalent. These should provide information and act as a guide to address:

- where appropriate, the duty to comply with the commitments set out in the WG “Duty to Share Personal Information”
- when and how consent should be obtained;
- the basic premise that individuals have the right to choose whether or not to agree to the disclosure of their personal information;

- the right of individuals to change their decision about a disclosure before it is made;
- When individuals make any decision to restrict disclosure of their personal information;
- who should obtain consent for further purposes;
- where and how consent or dissent should be recorded;
- answering questions about consent including how to provide information about the consequences of non-disclosure in a non-threatening, non-confrontational manner;
- how often consent should be reviewed;
- any sanctions for failure to respect individuals' disclosure decisions;
- other lawful reasons for disclosure of confidential personal information - public interest, legally required and section 251 of the NHS Act 2006.

8 Services Provided by Third Parties

Where an organisation contracts with a third party to provide care services for example Continuing Health Care the contracts must prevent personal information from being used for purposes other than those contracted for and must also ensure that there is explicit consent or some other lawful basis where required.

9 Data for publication

This is data that has been anonymised in line with the Information Commissioners Office anonymisation code to the point where determining individual identities from the data is unlikely, requiring unreasonable effort. The data does not require a legal or contractual basis for processing and can be publically disclosed. This data is called de-identified data for publication.