



DISCLOSURE OF PERSONAL DATA TO THE POLICE GUIDELINES

Reference No:	UHB 047	Version No:	UHB 1	Previous UHB / LHB Ref No:	T/138
----------------------	---------	--------------------	-------	-----------------------------------	-------

Documents to read alongside these guidelines	Data Protection Policy, Confidentiality: Code of Practice for Health and Social Care in Wales
---	---

Classification of document: Data Protection

Area for Circulation: UHB Wide

Author: Data Protection Manager

Executive Lead: Director of Innovation and Improvement

Group Consulted Via/ Committee: Medical Director, HR, Child Protection, Mental Health

Ratified by: Information Governance Committee

Date Published: 26th May 2011

Version Number	Date of Review	Reviewer Name	Completed Action	Approved By	Date Approved	New Review Date
UHB 1		Data Protection Manager	To replace Previous Trust Version 138	Information Governance Committee	26/04/2011	01/04/2014

Disclaimer

When using this document please ensure that the version you are using is the most up to date either by checking on the UHB database for any new versions. If the review date has passed please contact the author.

OUT OF DATE POLICY DOCUMENTS MUST NOT BE RELIED ON

CONTENTS	Page No.
1. Introduction	3
2. What is personal data?	3
3. Who should make a disclosure to the police?	3
4. Should I disclose personal data to the police?	3
4.1 Prevention of Terrorism Act	4
4.2 The Road Traffic Act	4
4.3 The Police and Criminal Evidence Act	4
4.4 Child Protection Legislation	4
5. Other circumstances where disclosure to the police is permitted	4
5.1 What to consider when deciding whether or not it is appropriate to disclose	5
5.2 Multiple Disclosures	5
5.3 Court Order	5
5.4 Coroners Court	6
5.5 Crime and Disorder Act	6
5.6 MAPPA	6
6. Important Notes	6
7. Transfer of personal data to the police	7
8. Equality Statement	7
Appendix 1	8

1. Introduction

These guidelines have been compiled to assist staff when dealing with police enquiries, where the personal data of an individual (patient, member of staff or the public) is requested.

2. What is Personal Data?

Data, including images, that is capable of identifying a living individual; it usually (but not exclusively) includes combinations of the following:

- Name
- Date of Birth
- Address and / or postcode
- Phone number
- Identity number (Hospital/NHS number, NI number etc.)
- Initials
- Gender

The physical or mental health or condition of a patient, member of staff or the public is classified as sensitive data under the Data Protection Act 1998 and as such, further consideration should be given to the appropriateness of any disclosures.

Under the Data Protection Act 1998, Human Rights Act 1998, Common Law and Caldicott Guidance you are under a duty to keep personal/sensitive information (about patients, staff and visitors) confidential and secure. There are however certain exemptions.

3. Who should make a disclosure to the Police?

Disclosures of personal information to the police should only be made by departmental managers, equivalent or more senior members of UHB staff. All disclosures must be recorded; including the reasons why you came to the decision to disclose.

The UHB Data Protection Manager should be consulted where there is any doubt regarding your ability in law to disclose. The Caldicott Guardian (Medical Director) will make the final decision in complex cases where patient identifiable data is involved.

4. Should personal data be disclosed to the police?

No...not unless that person or patient has given their consent, unless you believe that gaining consent would prejudice an investigation (e.g. evidence destroyed)

HOWEVER, there are circumstances where disclosures may be made. This section (4) deals with disclosures made by the UHB to the police and section 5 deals with disclosures where the police approach the UHB.

- 4.1 Prevention of Terrorism Act (1989) and Terrorism Act (2000)**
If you have gained information (including personal information) about terrorist activity you must inform the police.
- 4.2 The Road Traffic Act (1988)**
You have a statutory duty to inform the police, when asked, the name and address of any driver who is allegedly guilty of an offence under the Act; you should not disclose any clinical information
- 4.3 The Police and Criminal Evidence Act (1984)**
You may disclose but must consider the implications of gaining consent. You can pass on information to the police if you believe that someone may be seriously harmed or death may occur if the police are not informed. Serious arrestable offences are detailed in Appendix 1.
- 4.4 Child Protection Legislation**
Under section 47 of the Children Act (1989) a Local Authority must make enquiries (which might be through the police) necessary to decide whether they should take any action to safeguard or promote the child's welfare. In such a situation, firstly confirm it is a section 47 enquiry and then release relevant information, unless 'to do so would be unreasonable in the circumstances of the case'. You do not have to gain consent of the parent or child or inform them, however you may choose to if appropriate. NOTE; Seeking consent may prejudice a police investigation or may increase the risk of harm to the child.

If you suspect a child is being abused, but there is no request for information, you have a legal power to disclose information to Social Services (under 'vital interests' conditions of the Data Protection Act) and/or the police (under the Police and Criminal Evidence Act). Consider whether gaining consent or informing the child and parents would be beneficial or detrimental to the situation. If detrimental then disclosure without consent is permitted.

Always inform the UHB's Named Nurse for Safeguarding Children when disclosing information relating to children; tel. 20932628.

5. Other circumstances where disclosure to the Police is permitted

The police may seek personal data under an exemption in the Data Protection Act 1998 that permits the UHB to make a disclosure without the subjects consent. A section 29(3) exemption is used when making enquiries which are concerned with:

- a. the prevention and detection of crime, or**
- b. the apprehension or prosecution of offenders**

Police forces have standard forms for requesting personal data, in accordance with guidance issued by the Association of Chief Police Officers (ACPO). The form should certify that the information is required for an investigation concerning national security, the prevention or detection of crime, or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information.

The form must be signed by the senior officer in charge of the investigation.

NOTE; section 29(3) of the Data Protection Act allows you to disclose; **it does not require you to disclose.**

5.1 What to consider when deciding whether or not it is appropriate to disclose:

- Have the police indicated that informing the individual about the disclosure would prejudice their enquiry? If not, the individual should be informed of any disclosure.
- Without disclosure, would the task of preventing, detecting or prosecuting the crime be seriously prejudiced or delayed?
- Is the information limited to what is strictly relevant to a specific investigation? ('fishing trips' for non-specific information, not related to a specific incident are not the basis for disclosure of personal data)
- If the police state that the information is required 'in an emergency' and that they do not have their request in writing; record their name, rank and number, disclose the information and then contact the Officer's senior officer for the disclosure request to be put in writing.

You should not feel pressurised or intimidated into giving information just because the police have requested it, it is perfectly reasonable to ask why the information is needed and exactly what is required before deciding whether it is appropriate for information to be released.

5.2 Multiple Disclosures

There are times when you may release personal data relating to more than one person who the police do not name, but who fit a particular description. For example: the police may not have the name of the particular suspect, but they believe he is an employee (patient/visitor) of the UHB and have a particular description (for example, white male, between 20-30 with brown hair). In this situation, you may release the personal data of all employees who match that particular description.

5.3 Court Order

Where the Courts have made an order, you must disclose the required information, unless the UHB decides to challenge the Order at Court.

5.4 Coroners Court

The Coroner's Office may request a medical report in order to investigate the cause of death of a person in suspicious or unnatural circumstances. Information may be requested by a police officer on behalf of the Coroner; staff should confirm this with the Coroner's Office (tel. 20527431). Identification should be requested from the police officer and the officer's name, rank and number logged. A receipt for the record should be obtained from the police officer's property book.

5.5 Crime and Disorder Act (1998)

The police may seek information under section 115 of the Crime and Disorder Act 1998. Section 115 enables the disclosure, **but does not require the disclosure** of information for the purposes of any provision of the Crime and Disorder Act 1998. This means that, for example, information may be required on an individual 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. There may also be requests for aggregated data for detection, prevention or crime reduction purposes. **All disclosures under this Act must comply with the requirements of the Data Protection Act 1998.**

5.6 MAPPA

Section 325 Criminal Justice Act 2003 establishes a duty to co-operate with the Responsible Authority for Multi Agency Public Protection Arrangements (MAPPA). Co-operation may include the sharing of information but **any information shared must comply with other legal responsibilities such as the Data Protection Act 1998 and the Common Law Duty of Confidentiality.**

MAPPA assesses and manages the risks posed by violent and sexual offenders who may cause serious harm to the public.

The nature of any disclosure and the reasons for it must be noted clearly in the service user's record.

6. Important Notes:

- Always check the identity of anyone requesting information and only give the minimum information to satisfy the request.
- Where the subject has given consent to the release of their personal data, make sure you have proof of this.
- Seek advice when making a decision regarding disclosure and ensure you record your reasoning and any decisions made in the patient's health record or an employee's personnel file.

If you require advice or guidance regarding the disclosure of personal data, contact the UHB Data Protection Manager at: The PSA Building, University Hospital of Wales, tel: 2074 6677, e-mail nic.drew@ wales.nhs.uk

7. Transfer of personal data to the police

If you have been asked to provide personal data to the police by fax, you must follow the Safe Haven procedures in the UHB Data Protection Policy, section 11. If you have been asked to provide personal data in an electronic format (e.g. CD/DVD, memory stick), you must follow the procedure in the UHB Data Protection Policy, Appendix 7, section 5 – all electronic disclosures **MUST** be encrypted. **NOTE; disclosures to the police by email are not permitted.**

8. Equality Statement

We have undertaken an Equality Impact Assessment and received feedback on this guidance and the way it operates. We wanted to know of any possible or actual impact that this guidance may have on any groups in respect of gender, race, disability, sexual orientation, Welsh language, religion or belief, transgender, age or other protected characteristics. The assessment found that there was no impact to the equality groups mentioned. Where appropriate we have taken the necessary actions required to minimise any stated impact to ensure that we meet our responsibilities under the equalities legislation.

APPENDIX 1

Disclosing in connection with a serious crime

Disclosing information to help prevent, detect or prosecute serious crime may sometimes be justified to protect the public. Although there is no absolute definition of serious crime, Section 116 of the Police and Criminal Evidence Act 1984 identifies some serious arrestable offences which include:

- Treason
- Murder
- Manslaughter
- Rape
- Kidnapping
- Certain sexual offences
- Causing an explosion
- Certain firearm offences
- Taking of hostages
- High jacking
- Causing death by reckless driving
- Offences under prevention of terrorism legislation

Also, making a threat which if carried out would be likely to lead to:

- A serious threat to the security of the state or to public order
- Serious interference with the administration of justice or with the investigation of an offence
- Death or serious injury