



British Paediatric Surveillance Unit of the Royal  
College of Paediatrics and Child Health

## Understanding data confidentiality and security within a BPSU surveillance study

Royal College of Paediatrics and Child Health, 5-11 Theobalds Road, London WC1N 8SX  
Tel: (020) 7 092 6173/4      Fax: (020) 7 092 6001      Email: [bpsu@rcpch.ac.uk](mailto:bpsu@rcpch.ac.uk)

## Part A: Applying to the BPSU

### The British Paediatric Surveillance Unit (BPSU) and Patient Confidentiality

In order to apply for ethical approval and for approval to collect surveillance data from individual patients without their consent, it is important to understand the legal framework governing BPSU studies.

This document summarises the laws applying to BPSU surveillance studies and the necessary approvals that are required before a study can commence.

#### Summary

##### The BPSU requires study applicants to

- apply to the **Ethics and Confidentiality Committee of the National Information Governance Board** for approval under Section 251 of the NHS Act 2006 (to collect personal data about NHS patients without their consent)
- demonstrate compliance with the eight principles of the **Data Protection Act 1998**
- demonstrate compliance with the principles of the **Caldicott Report (1997)**
- detail measures to protect patient confidentiality and data security.

## **Part A: Applying to the BPSU**

### **1. Background to medical confidentiality as applied to BPSU studies**

In the UK there are a number of pieces of legislation that address confidentiality of personal information. These include Common Law, the Data Protection Act 1998, the Human Rights Act 1998 and the NHS Act 2006.

#### **1.1 Common Law**

In Common Law anyone who receives information must respect its confidentiality i.e. not disclose it without consent or other strong justification. A principle of Common Law is that confidential information about a living person should not be disclosed without their consent. Information that doctors have about their patients is regarded as confidential. However, Common Law also recognises that it can be in the public interest for doctors to disclose confidential personal information and that such disclosure should be balanced against the benefits to society. Common Law establishes core principles but does not specify situations where confidential information may or may not be disclosed.

#### **1.2 Data Protection Act 1998<sup>1</sup>**

If a living person (data subject) can be identified from a set of data, these are considered personal data. Within the context of a BPSU study, identifiable information may include names, addresses, initials, sex, date of birth and/or death, the rare disorder name, postcode and ethnicity. Personal data stored in computers and/or paper files (ward notes, X-rays, lab reports etc) is safeguarded by the Data Protection Act 1998.

The eight principles of the Data Protection Act are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met; and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

---

<sup>1</sup> Available at <http://www.opsi.gov.uk/acts/acts1998/19980029.htm>

## **Part A: Applying to the BPSU**

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

### **1.3 Human Rights Act<sup>2</sup>**

The Human Rights Act 1998 allows UK citizens to assert their rights under the European Convention on Human Rights in UK courts. The European Convention on Human Rights, includes the right to respect for individual private lives and lays down circumstances in which it is legitimate for a public authority to interfere with this right, for example for public good.

### **1.4 Caldicott Report**

The Caldicott Report (1997) was a review commissioned by the Chief Medical Officer. The Caldicott Committee reviewed data confidentiality and flows of data throughout the NHS. The Caldicott Report identified six principles for using patient identifiable data (data from which individual NHS patients might be identified).

1. Justify the purpose(s) for using patient data
2. Don't use patient-identifiable information unless it is absolutely necessary
3. Use the minimum necessary patient-identifiable information
4. Access to patient-identifiable information should be limited to as few people as possible
5. Everyone should be aware of their responsibilities to maintain confidentiality
6. Data practices should comply with the law, in particular the Data Protection Act.

### **1.5 NHS Act 2006**

The NHS Act 2006 established the **National Information Governance Board (NIGB)** as a statutory body whose functions include the approval for studies using patient identifiable data without individual consent, under Section 251 of the Act. A specific committee, the Ethics and Confidentiality Committee (ECC), reviews and approves applications for approval on behalf of the NIGB. (This function was formerly performed by the Patient Information Advisory Group (PIAG) which was established under the Health and Social Care Act 2001 but disbanded when the NIGB came into being.)

---

<sup>2</sup> Available at <http://www.opsi.gov.uk/acts/acts1998/19980042.htm>

## **Part A: Applying to the BPSU**

Section 251 recognises that there are essential activities of the NHS, such as cancer registries and medical surveillance research, that require use of identifiable patient information without patient consent. Section 251 only approves applications that are in the interests of patients or the wider public, when consent is not practicable and anonymised information will not suffice.

The terms of reference, membership and application procedures of the ECC can be found on their website (see below).

### **Differences in Scotland and Northern Ireland**

#### **1.6 Privacy Advisory Committee (PAC)**

NIGB approval for data collection without consent does not apply in Scotland and Northern Ireland. In these countries, ethics approval is sufficient. However, if data from the Information and Statistics Division (ISD) of the Scottish NHS is being used without individual consent, then the Privacy Advisory Committee will review and advise the ISD on the application. The PAC is already established in Scotland and in the process of being established in Northern Ireland. It is not the Scottish equivalent of the NIGB and there is no requirement for BPSU studies to be approved by the PAC.

### **Other resources to help understand the UK information governance framework**

#### **1.7 NHS Information Governance toolkit**

NHS Connecting for Health has devised a 'toolkit' to help researchers understand the information governance, and particularly the requirements for data security and confidentiality, within NHS clinical care and research using NHS data. A weblink is provided below.

#### **1.8 MRC Data and Tissue toolkit**

The Medical Research Council (MRC) has produced a toolkit guide to using patient data and tissue within research studies. They had produced a 'toolkit' which provides an overview or 'roadmap' of current UK frameworks for protecting patient data confidentiality. A weblink is provided below.

Part B: **Abbreviations and useful weblinks for further information:**

<b>Abbreviation</b>		<b>Weblinks</b>
<b>ECC</b>	Ethics and Confidentiality Committee (of the NIGB)	<a href="http://www.nigb.nhs.uk/ecc">www.nigb.nhs.uk/ecc</a>
<b>NIGB</b>	National Information Governance Board	<a href="http://www.nigb.nhs.uk">www.nigb.nhs.uk</a>
<b>PAC</b>	Privacy Advisory Committee (Scotland and Northern Ireland only)	<a href="http://www.isdscotland.org/isd/3048.html">www.isdscotland.org/isd/3048.html</a>
<b>PIAG</b>	Patient Information Advisory Group (role taken over by ECC)	<a href="http://www.advisorybodies.doh.gov.uk/PIAG/Index.htm">www.advisorybodies.doh.gov.uk/PIAG/Index.htm</a>
<b>SLSP</b>	System Level Security Policy	<a href="http://www.nigb.nhs.uk/ecc/applications/SLSP.doc/view?searchterm=slsp">www.nigb.nhs.uk/ecc/applications/SLSP.doc/view?searchterm=slsp</a>
<b>Other useful weblinks</b>		
<b>NHS Information Governance Toolkit (Connecting for Health)</b>		<a href="http://www.igt.connectingforhealth.nhs.uk/">www.igt.connectingforhealth.nhs.uk/</a>
<b>MRC Data and Tissue Toolkit</b>		<a href="http://www.dt-toolkit.ac.uk/home.cfm">www.dt-toolkit.ac.uk/home.cfm</a>
<b>Data Protection Act 1998</b>		<a href="http://www.opsi.gov.uk/acts/acts1998/19980029.htm">www.opsi.gov.uk/acts/acts1998/19980029.htm</a>
<b>Human Rights Act 1998</b>		<a href="http://www.opsi.gov.uk/acts/acts1998/19980042.htm">www.opsi.gov.uk/acts/acts1998/19980042.htm</a>
<b>NHS Act 2006</b>		<a href="http://www.opsi.gov.uk/acts/">www.opsi.gov.uk/acts/</a>
<b>MRC Personal Medical Information Guidance</b>		<a href="http://www.mrc.ac.uk/pdf-pimr.pdf">www.mrc.ac.uk/pdf-pimr.pdf</a>