

Regulation of Investigatory Powers Act 2000

April 2009

NHS Bolton is the name used to refer to Bolton Primary Care Trust. The legal identity of the organisation remains unchanged.

Document control

Doc. Ref. No.	IMTDP005
Title of document	Regulation of Investigatory Powers Act 2000
Author's name	Penny Baxter
Author's job title	Data Protection Manager
Dept / Service	IM&T
Doc. Status	V1.2
Based on	RBH policy (Author Jean Gleave)
Signed off by	IM&T Strategy Group
Original Publication Date	September 2004
Last Review Date	April 2009
Next review date	April 2011
Distribution	All PCT staff

Contents

1	INTRODUCTION.....	4
2	PRINCIPLES.....	4
3	AUTHORISATION.....	5
3.1	Applications for directed surveillance	6
3.2	Information to be supplied	6
4	PROCEDURE.....	7

The regulation of Investigatory Powers Act 2000 (RIPA)

1 Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) came into force on 28th July 2000. The Act makes certain requirements of public bodies who may consider undertaking covert surveillance operations. Prior to RIPA there was no regulation of public authorities in their use of surveillance. RIPA seeks to address this and to ensure that any surveillance activities undertaken are properly regulated and comply with the Human Rights Act 1998. Codes of Practice have been produced to give guidance in the application of the Act, and the surveillance Commissioners and the Surveillance Tribunal have been set up as a mechanism for oversight and redress.

The NHS needs to pay heed to RIPA and the Codes of Practice, as failure to do so may lead to the exclusion of evidence from a hearing and may enable a defendant to take action against the PCT, through the civil courts, for breach of Human Rights.

Full details of the Act can be obtained from the web site:

www.hms0.gov.uk/acts/acts2000

2 Principles

The Act contains five parts:

Part I	Interception of communications
Part II	Surveillance and Covert Human Intelligence Sources
Part III	Investigation of Electronic Data protection by encryption
Part IV	A Framework for Scrutiny of Investigatory Powers
Part V	Miscellaneous (Interference with Property & Wireless Telegraphy)

The Act covers two types of surveillance:

1. Intrusive Surveillance – covert surveillance carried out in relation to residential premises or a vehicle. This can only be carried out by police, Customs and Excise and the security services.

2. Directed Surveillance – this can be undertaken by public authorities provided that an assurance is given that no surveillance will be undertaken without obtaining the authority of the designated officer.

Directed surveillance is defined as surveillance which is covert but which is not intrusive and which is undertaken:

- For a specific investigation
- In a manner likely to obtain private information about a person

Covert surveillance is surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

Schedule 1 to the Act notes that Health Authorities, Special Health Authorities and NHS Trusts are relevant authorities for purposes of certain elements of part II of the Act.

3 Authorisation

All authorisations must be given in writing:

- Fraud related cases must be referred to the Directorate of Counter Fraud Services (DCFS) for authorisation.
- Non-fraud related cases e.g. theft must be referred to the Chief Executive for authorisation.

Surveillance activity can only be lawfully authorised if its purpose is for one of the following reasons:

- To prevent or detect crime
- In the interest of public safety
- For the purpose of protecting public health
- For the purpose of assessing or collecting any tax, levy or other imposition, contribution or charge payable to a government department

There are other reasons which are outside the scope of the NHS:

- In the interest of National Security
- In the interests of the economic well-being of the United Kingdom

In urgent cases authorisation can be given orally – in such cases a statement that the authorising officer has expressly authorised the action should be recorded in writing as soon as is reasonably practicable, and endorsed by the authorising officer. Authorising officers should not be responsible for authorising their own activities.

Written authorisation will cease to have effect (unless renewed) at the end of a period of 3 months. Urgent oral authorisations (or written authorisations granted by a person who is only entitled to act in urgent cases) will cease to have effect (unless renewed) after 72 hours.

3.1 Applications for directed surveillance

- Must be on a prescribed form
- Must be for a prescribed purpose
- Must be proportionate to what is sought to be achieved
- Must be necessary
- Must have consideration to collateral intrusion (effect on 3rd parties)
- Must be planned and
- Authority given in writing (can be verbal authority if urgent)

3.2 Information to be supplied

- Action to be authorised – including any premises or vehicles involved
- Identities of those involved – where known
- An account of the investigation – a summary of the investigation to give the Chief Executive the information required in order to demonstrate proportionality
- Grounds for authorisation – i.e. for detection of a crime etc.,
- What information is to be obtained – i.e. the intention of the operation
- The potential for collateral intrusion – i.e. what impact there will be on third parties
Include details of action taken to minimise this.
- Religious and confidential material – an assessment of the likelihood of this type of material being discovered should be described. Guidance relating to religious and confidential material is set out in paragraphs 2.8 to 2.11 of the Code of Practice.

4 Procedure

Any requests for the use of surveillance activities should be directed, in the first instance, to the PCTs nominated Local Counter Fraud Specialist (LCFS). This officer will assess the information and discuss the case with the Regional Operation Counter Fraud Manager. For fraud related cases the LCFS will make the required application to the relevant officer through the Counter Fraud Service authorisation procedure.

Within the PCT it is only the Chief Executive (or the person nominated to carry out their lawful functions in their absence) who can authorise the activity in relation to non-fraud and corruption matters.