CARD 3
Sources of confidentiality rights and protections

It is important to note that the ethical, professional, contractual and legal positions on confidentiality are complex. For example, the legal responsibilities in respect of confidential information cannot be gleaned from common law and statute alone, and health professionals must look at the overall effect of the law, not each aspect in isolation. In terms of statute, the Data Protection Act sets out circumstances in which the use of data may be lawful. The common law generally requires consent for disclosure. Health professionals must be sure that any use of data falls into the relevant Data Protection Act categories and meets the common law requirement for consent except where disclosures are required by law or in the public interest. Health professionals who are uncertain about the application of the law should seek legal advice. They must also ensure that their actions comply with the guidance issued by their regulatory body and their employers.

The use of information about individual patients is governed by the following:

1. **Contract of employment**
   Confidentiality of patient information is a requirement of employment under NHS and many independent sector contracts. All staff employed by or contracted to the NHS may be disciplined following a breach of patient confidentiality.
2. Professional standards
All health care professionals must maintain the standards of confidentiality laid down by their professional body, such as the GMC, or risk complaint for professional misconduct. This may result in a warning, restriction of practice or removal from the register. (See also Card 1: ‘GMC’.)

3. Policies and organisational standards
A wide range of policies and standards exist which provide guidance for health professionals to ensure that patients are fully involved with decisions about the use of their information and that information provided by patients is kept confidential. This includes the Caldicott Guardian Manual (2006), the Department of Health Confidentiality: NHS Code of Practice (2003), the Scottish Government Health Directorates NHS Code of Practice on Protecting Patient Confidentiality (2003), and the Northern Ireland Code of Practice on Protecting the Confidentiality of Service User Information (awaiting publication).

4. NHS Care Record Guarantee
The NHS Care Record Guarantee emphasises the commitment of the NHS in England to the confidentiality and security of patient information. The guarantee covers:
• patients’ access to their own records
• controls on access by others
• how access will be monitored and policed
• options patients have to further limit access
• access in an emergency
• what happens when patients cannot make decisions for themselves.
5. **Data Protection Act 1998**
The Data Protection Act regulates the processing of information about living individuals, such as obtaining, use or disclosure of information. It covers paper and computer records. Patients are entitled to be informed that information is being held about them and of the purposes for which their information will be processed. They are entitled to have access to and a copy of their information, except where there are grounds for believing that access to that information would be likely to cause serious harm to the individual or a third party or where it would entail disclosure of another individual’s identifiable data. They are also entitled to have information corrected when it is inaccurate. (See also Card 1: ‘IC’ and ‘Access’.)

The Data Protection Act does not cover the records of deceased patients. Statutory rights of access are contained within the Access to Health Records Act 1990 and Access to Health Records (Northern Ireland) Order 1993. A personal representative or any person with a claim arising from the death of a patient has a right of access to information directly relevant to the claim. Information which is not directly relevant to the claim may not be released. (See also Card 1: ‘Access’.)
A right to ‘respect for private and family life’ is guaranteed in article 8 of the Human Rights Act (HRA). This right is not absolute, and may be derogated from where the law permits and ‘where necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’. The effect is similar to that of the common law: privacy is an important principle which must be respected, but may be breached where other significant interests prevail. Any such breach must be proportionate to the benefits/harms it is intended to bring/avoid. (See also Card 1: ‘HRA’.)

It is an offence under the Act to gain unauthorised access to computer material. This would include using another person’s ID and password without authority in order to use, alter or delete data.

In England and Wales, Section 251 of the NHS Act 2006 gives the Secretary of State for Health power to make regulations permitting the disclosure of identifiable information without consent in certain circumstances. Health professionals can apply to the Ethics and Confidentiality Committee (ECC), an independent public body which advises the Secretary of State for Health in England and Wales about the lawful basis for disclosure of patient-identifiable information. (See also Card 1: ‘ECC’.)
10. The common law

The common law is based on previous judgments in court. Whilst various interpretations of the common law may be possible, there is widespread acceptance that it reinforces the view that information may be disclosed with patient consent, where there is an overriding public interest or where the law requires it. (See also Card 9 on Legal and Statutory Disclosures and Card 10 on Public Interest.)