Data misuse and the health professional regulators
(ID 21/2008)
July 2009

Executive summary

1. CHRE have been asked by the Secretary of State to provide advice about the current codes of conduct for the regulated healthcare professions around data misuse.

2. Patients' personal data is at the heart of healthcare. Patients consent to share their personal medical data with professionals. In turn this drives diagnosis and treatment, plays a key role in aiding the delivery of care, allows a record of an individual's medical history to be built up, and supports patient safety. The sensitive nature of personal information places obligations and duties on health professionals to ensure that when data are recorded, stored, shared and accessed this is done in accordance with legal and ethical standards and requirements.

3. The confidentiality and security of patients' data is a core value for all health professionals and this is reflected in all regulators' core codes and standards. Some regulators also issue supplementary guidance to help registrants manage patients' information in particular situations they may encounter in the course of their practice. Standards and codes of conduct are generally reviewed and updated on a five yearly basis. However, immediate updates are made if changes are made to wider legislation.

4. Other legal duties govern health professionals' use of patients' data. These include obligations such as those laid down by the Data Protection Act 1998, the Human Rights Act 1998, and the common law of confidentiality. This is as well as guidance provided by professional bodies and employing organisations such as the NHS. These sources are cross-referenced in regulators' standards and codes.

5. The advent of new forms of data storage and management present different risks around data misuse. The regulators shared a view that different methods of storing or handling personal data in healthcare settings did not require different approaches to standards or fitness to practise.

6. It is difficult to identify trends in complaints to regulators about this issue. The number of cases involving data misuse is often small and some regulators do not record this level of detail of subject of complaints for further analysis. Furthermore, charges relating to the misuse of patients' data may be considered alongside other unrelated charges. Each series of charges is therefore unique and the circumstances and evidence equally individual. Even when misconduct may be found, the sanction that may be applied can be influenced by a registrant demonstrating insight and awareness of their actions.

7. However, we have to accept and anticipate changing views and expectations among the public about the confidentiality and security of their data, both in healthcare and more widely. When regulators provide guidance to registrants it is essential that changes in the public's expectations around these issues are noted and reflected, as well as new legal requirements or challenges that emerge from innovative use of

information technology. The principles embedded in regulators' codes and standards about confidentiality and security are neutral in terms of practice settings. However, their interpretation by health professionals has to be contemporary and respond to new risks and expectations, as well as established threats. Additional guidance from regulators is welcome to support professionals' practice, especially when these circumstances change. Assessments of complaints about fitness to practise should reflect the circumstances of the alleged misconduct, and we believe this should include consideration of the public's current expectations of professionals' handling of their personal data.

Introduction

1. The Council for Healthcare Regulatory Excellence (CHRE) is an independent body accountable to Parliament. Our primary purpose is to promote the health, safety and well-being of patients and other members of the public. We scrutinise and oversee the health professional regulatory bodies[1], work with them to identify and promote good practice in regulation, carry out research, develop policy and give advice.

2. Under section 26A of the National Health Service and Health Profession Reform Act 2002, we have been asked by the Secretary of State to provide advice about the current codes of conduct for the regulated healthcare professions around data misuse. In particular we have been asked to:

'work with Professional Regulation bodies to provide clarification about personal misconduct in relation to data misuses and transparency in relation to how these issues are reported in particular, by providing advice on the following:

- *The extent to which they reflect the information governance requirements that now prevail within the NHS;*
- *Suggestions to whether these codes of conduct might need reviewing so that they more adequately (if required) reflect the information governance requirements in relation to electronic information relating to patients and staff; and any role the Department might play in such reviews; and*
- *If it would be feasible or desirable to incorporate into definitions of misconduct the responsibilities of all parties in relation to electronic person identifiable data.'*

3. This report provides our response to this request. In preparing our response we have considered the standards registrants are expected to demonstrate and the regulators' management of fitness to practise issues that can arise when registrants fail to meet these standards. First we describe the current approaches taken in regulators' codes of conduct around data misuse. We then consider these approaches in relation to other information governance requirements that prevail in healthcare. Finally we consider misconduct around data handling, how it is managed by the regulators, and discuss whether changes are necessary. Appendix 1 outlines current standards and guidance from regulators relating to data misuse.

4. In considering the Secretary of State's questions, we asked the health professional regulatory bodies the following questions.
   - In your view, do different methods of storing and handling personal data in healthcare settings demand different approaches to standards and fitness to practise?
   - Are you aware of any trends in your fitness to practise cases involving data security issues?
   - What guidance and training do you provide to fitness to practise (FTP) panellists on the issues of data misuse and data security?
   - How often do you update your guidance to a) registrants and b) FTP panellists in this area?

[1] The regulatory bodies we oversee are: General Chiropractic Council, General Dental Council, General Medical Council, General Optical Council, General Osteopathic Council, Health Professions Council, Nursing and Midwifery Council, Pharmaceutical Society of Northern Ireland, Royal Pharmaceutical Society of Great Britain

Personal data in healthcare

5. Patients' personal data is at the heart of healthcare. Patients consent to share their personal medical data with professionals. In turn this drives diagnosis and treatment, plays a key role in aiding the delivery of care, allows a record of an individual's medical history to be built up, and supports patient safety. The sensitive nature of personal information places obligations and duties on health professionals to ensure that when data are recorded, stored, shared and accessed this is done in accordance with legal and ethical standards and requirements.

6. The confidentiality of patients' data is a core value for all health professionals. This is reflected in the prominence given to this issue in the Chief Executives' statement on common values for health professionals: 'Keep information about patients and clients confidential'.[2]

7. Through their core standards and codes of conduct and practice, each regulator describes the expectations of registrants when they handle personal data. The topics covered are recording information, maintaining confidentiality and security, and how and when information may be released, with and without consent. These standards apply wherever a health professional is practising. Some regulators also issue supplementary guidance to help registrants manage patients' information in line with current legal and ethical requirements. The following is a list of relevant current standards and guidance documents for registrants provided by the health professional regulators:

General Chiropractic Council (GCC)	*Code of practice and standard of proficiency* (2005; revised version in 2010)
General Dental Council (GDC)	*Standards for dental professionals* (2005) *Principles of patient confidentiality* (2007)
General Medical Council (GMC)	*Good medical practice* (2006) *Confidentiality: protecting and providing information* (2004; revised version due late 2009)
General Optical Council (GOC)	*Code of conduct for individual registrants* (2005) *Code of conduct for business registrants* (2005)
General Osteopathic Council (GOsC)	*Code of practice* (2004)
Health Professions Council (HPC)	*Standards of conduct, performance and ethics* (2008) *Guidance on confidentiality* (2008)
Nursing and Midwifery Council (NMC)	*The Code: Standards of conduct, performance and ethics for nurses and midwives* (2008) *Confidentiality advice sheet* (2009) *Record keeping: guidance for nurses and midwives* (2009)
Pharmaceutical Society of Northern Ireland (PSNI)	*Code of ethics* (2009) *Professional standards and guidance for patient confidentiality* (2009)

[2] Common Values Statement by the Chief Executives Group of the Health Care Regulators on professional values. 2006. Available at: http://www.chre.org.uk/_img/pics/library/Common_values_statement.pdf [accessed 3 July 2009]

Royal Pharmaceutical Society of Great Britain (RPSGB)	*Code of Ethics* (2007) *Professional standards and guidance for patient confidentiality* (2007)

8. Standards and codes of conduct are generally reviewed and updated on a five yearly basis. However, when regulators' guidance in this area reflects and incorporates wider legal duties, more immediate updates are made when legislation changes.

9. We recognise that health professionals will also handle personal data as they fulfil other roles such as managers, employers, or business registrants. Some regulators have provided guidance to their registrants about the management of non-clinical, personal data about staff or clients that is not specifically about clinical or medical needs. For example:

   'You must, as appropriate to your particular management responsibilities, ensure that: …procedures respect and protect confidential information about patients and employees in accordance with current legislation, relevant codes of practice and professional guidelines.' (RPSGB) [3]

   '… chiropractors should make sure that if they employ a bookkeeper or an accountant then financial information on payments can be looked at separately from clinical records. Secondly, if a chiropractor wishes to pursue a patient for overdue payments, then only the minimum information for the situation in hand should be supplied to outside bodies (eg for legal proceedings or for debt collection). Thirdly, for chiropractors thinking of selling their business there is a need to gain the patients' specific consent to the transfer of their records as otherwise their confidentiality could be compromised.' (GCC) [4]

   'If you have wider responsibilities for consent and confidentiality issues within your organisation you should keep up to date with and observe the legal and ethical guidelines on handling confidential information, with particular reference to the Data Protection and Freedom of Information Acts.' (GMC) [5]

10. While not directly relevant to the commission's interest in the codes of conduct issued by regulators' to registrants, it is important to acknowledge that sensitive personal data from patients can form part of evidence in regulators' fitness to practise cases and it is essential that it is handled appropriately. The guidance and training provided to panellists focuses on their duties as panellists to ensure data are protected while panellists discharge their duties. The NMC told us that 'Confidentiality is a key theme in FTP panellist training' and the PSNI ensured specialists training by an external consultant 'which includes elements related to data misuse and security'. The RPSGB provided panellists with data protection guidance in November 2008.

11. In preparing this advice we have focused on patients' clinical records and misuses that can arise from this in the course of providing healthcare. We have not considered potential secondary uses of patients' data, for example in research, although misuse

[3] RSPGB, 2007. Professional Standards for Pharmacists and Pharmacy Technicians in Positions of Authority. Available at: http://www.rpsgb.org/pdfs/coepsposauth.pdf [accessed 3 July 2009]
[4] GCC, 2005. Code of practice and standard of proficiency. Available at: http://www.gcc-uk.org/files/link_file/COPSOP_Dec05_WEB(with_glossary)07Jan09.pdf [accessed 3 July 2009]
[5] GMC, 2006. Management for Doctors. Available at: http://www.gmc-uk.org/guidance/current/library/management_for_doctors.asp [accessed 3 July 2009]

and misconduct may occur in these situations. Our emphasis on use of data in delivery of healthcare does not deny the important issues around management of non-clinical, personal data such as payroll, references and financial arrangements with clients and business partners. This focus allows us to concentrate on the particular specifics of managing the security and confidentiality of personal medical information that is distinctive to the working circumstances of health professionals.

Other standards, codes and guidance

12. Alongside the standards set by regulators, other legal duties govern health professionals' use of patients' data. These include obligations such as those laid down by the Data Protection Act 1998, the Human Rights Act 1998, and the common law of confidentiality. This is as well as guidance provided by professional bodies and employing organisations such as the NHS. These sources are cross-referenced in regulators' standards and codes. For example, the RPSGB state:

    'This document does not detail specific legal requirements, but you must ensure you comply with relevant legislative requirements set out in the Data Protection Act and associated legislation, as well complying with common law principles and with any NHS or employment policies that may apply to your work.' [6]

    In England, further details of the full range of requirements covering this area can be found in the Department of Health publication *NHS information governance – guidance on legal and professional obligations.*[7]

13. Professional organisations also provide guidance in various aspects of these matters. These are explicitly referenced in the GOC codes of conduct, as individual and business registrants are expected to refer to guidance published by professional bodies such as the College of Optometrists and the Association of British Dispensing Opticians.[8]

14. Regulators of health and social care services place obligations on service providers around the management of records. For example, the Care Quality Commission, the service regulator in England, is working with the following draft regulations for registration:

    Regulation 18 – Records
    18.—(1) The registered person must ensure that service users are protected against the risks of unsafe or inappropriate care and treatment arising from a lack of proper information about them by means of the maintenance of—
    (a) an accurate record in respect of each service user which shall include appropriate information and documents in relation to the care and treatment provided to each service user; and

[6] RPSGB, 2007. Professional Standards and Guidance for Patient Confidentiality. Available at: http://www.rpsgb.org/pdfs/coepsgpatconf.pdf [accessed 3 July 2009]
[7] Department of Health, 2007.NHS information governance – guidance on legal and professional obligations. Available at: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616 [accessed 26 June 2009]
[8] GOC Code of conduct for individual registrants. http://www.optical.org/goc/filemanager/root/site_assets/codes_of_conduct/code_registrants.pdf [accessed 30 June 2009]

(b) such other records as are appropriate in relation to the carrying on of the regulated activity.
(2) The registered person must ensure that the records referred to in paragraph (1) (which may be in paper or electronic form) are—
(a) kept securely and can be located promptly when required;
(b) retained for an appropriate period of time; and
(c) subject to sub-paragraph (b), securely destroyed when it is appropriate to do so.
(3) In deciding what records are appropriate for the purposes of paragraph (1)(b), and for how long such records should be retained for the purposes of paragraph (2)(b), the registered person must have regard to guidance issued by the Commission.[9]

15. Across the UK, NHS organisations are expected to follow national codes of practice as part of wider information governance frameworks. For example in England, the NHS Information Governance Standard provides a framework under four headings – management and accountability, process, people, assessment and audit. Within 'Process', reference is made to guidance in the form of three existing NHS Codes of practice – Confidentiality, Information Governance, and Records Management – and the NHS Care Record Guarantee.[10] The administrations in Northern Ireland, Scotland and Wales also have codes of practice around confidentiality as part of national information governance policies.[11] These are similar in form and content to the codes and standards outlined by the health professional regulators.

16. Together these codes, standards, policies and governance frameworks provide a matrix of assurance for the management of patients' information. They share principles, policies and good practice around records management, information security, and confidentiality in healthcare settings. Given the considerable overlapping interests in this area there could be a threat of guidance overload, so joint ventures are welcome. The GMC described work they have undertaken with the Information Commissioner and the DH in England on the use of IT equipment and access to patient data.[12]

Taking action against incidents of data misuse

17. Misuse of patients' information can take many forms. For example, discussing confidential information in earshot of third parties, deletion of records, not locking filing cabinets, or the unsecure disposal of records. Media reports of breaches of security and confidentiality include the following:

---

[9] Care Quality Commission, 2009. Consultation on new registration standards. Available at: http://www.cqc.org.uk/getinvolved/consultations/consultationonnewregistrationstandards.cfm [accessed 29 June 2009]

[10] Draft IG standard published in IGAP closure document Appendix 2 http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igap/igapclosure.pdf [accessed 29 June 2009]

[11] Department of Health, Social Services and Public Safety, Northern Ireland, 2009. Code of practice on protecting the confidentiality of service user information Available at: http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf [accessed 3 July 2009]; NHS Scotland Code of Practice on Protecting Patient Confidentiality, 2004; NHS Wales, 2005. Confidentiality Code of Practice for Health and Social Care in Wales. Available at: http://wales.gov.uk/docrepos/40382/4038212/403821/4038211/4038211/CodeofPractice?lang=en [accessed 3 July 2009]

[12] GMC, DH, ICO. Joint guidance on use of it equipment and access to patient data. Available at: http://www.gmc-uk.org/guidance/news_consultation/Joint_guidance_on_use_of_IT_equipment.pdf [accessed 30 June 2009]

- Theft of records from a maternity hospital, containing mothers' names, date of caesarean section, time of birth[13]
- Theft of a laptop carrying unencrypted data of around 5000 patients and loss of a memory stick containing unencrypted data about patients and staff[14]
- A survey of a London teaching hospital found that among 105 doctors, 92 carried memory sticks, 79 held confidential patient data on memory sticks, only five were password protected. The researchers found that the memory sticks were, 'usually attached to keys or ID badges carried inside and outside hospitals. They could be easily mislaid.'[15]

18. The advent of new forms of data storage and management may present different risks around data misuse. The regulators shared a view that different methods of storing or handling personal data in healthcare settings did not require different approaches to standards or fitness to practise:

    '… fitness to practise procedures are based on the principles set out in the guidelines. The individual circumstances of a case may need to be considered, but standards should remain consistent.' (GMC)

    'The existing guidelines for record keeping for nurses and midwives assert that the principles of good record keeping apply to all types of records.' (NMC)

    'The minimum standards of data protection should remain the same regardless of how the data is stored or handled.' (RPSGB)

    'The obligations of protecting data are the same regardless of data format, and different methods are not necessary.' (GDC)

    A similar sentiment is reflected in the guidance on confidentiality for health and social care staff working in Northern Ireland:

    'Service users' right to privacy and the staff's duty to confidentiality apply regardless of the form in which information is held or communicated, for example electronic, paper, photographic or biological.'[16]

19. Fitness to practise proceedings arise from complaints raised with regulators when conduct has fallen below the standards expected and sufficient evidence being available for the regulator to take a case to a hearing before an independent panel. When this does occur, charges relating to the misuse of patients' data may be considered alongside others. Each series of charges is therefore unique and the circumstances and evidence equally individual. Even when misconduct may be found, the sanction that may be applied can be influenced by a registrant demonstrating insight and awareness of their actions.

---

[13] 2009. Baby records theft sparks inquiry. *BBC News*, 11 May 2009. Available at: http://news.bbc.co.uk/1/hi/scotland/north_east/8043566.stm [accessed 29 June 2009]
[14] West, D, 2009. Trusts breached patient data protection rules. *Health Service Journal*, 29 Jan 09 http://www.hsj.co.uk/trusts-breached-patient-data-protection-rules/1973988.article [accessed 29 June 2009]
[15] Putnis, S, Bircher A, 2008. Data protection in the NHS - a ticking time bomb? *Health Service Journal* 4 September 2008. Available at: http://www.hsj.co.uk/data-protection-in-the-nhs-a-ticking-time-bomb/1832759.article [accessed 29 June 2009]
[16] Department of Health, Social Services and Public Safety, Northern Ireland, 2009. Code of practice on protecting the confidentiality of service user information Available at: http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf [accessed 3 July 2009];

20. It is difficult to identify trends in complaints to regulators about this issue. The number of cases involving data misuse is often small and some regulators do not record this level of detail of subject of complaints for further analysis.
    - The HPC reported a small number of cases each year
    - The NMC told us they are not aware of any trends with cases relating to data security issues, though some cases may have data misuse encompassed as part of the wider charges in a case
    - The RPSGB reported that 'from general experience the most visible trend involving data security issues related to the management of patient medication records in community pharmacy'
    - The PSNI reported a case where patient's information was misused by a professional to obtain controlled drugs by deception
    - The GCC described cases where registrants were reported to be discussing patient information in inappropriate circumstances, or not locking filing cabinets that contained sensitive information.

21. From our database of fitness to practise determinations, there have been few cases involving data misuse (approximately 20 out of a total of around 3000 since 2006). Drawing robust conclusions from this small number is not possible as the circumstances of each instance were different.

Discussion

22. Data misuse is clearly a live issue for the healthcare sector and concerns have been expressed by some about how well personal data is protected. For example, in April 2009 the Information Commissioner called on the NHS to handle sensitive patient information with the right level of security:

    'It is a matter of significant concern to us that in the last six months it has been necessary to take regulatory action against 14 NHS organisations for data breaches. In these latest cases staff members have accessed patient records without authorisation and on occasions, have failed to adhere to policies to protect such information in transit. There is little point in encrypting a portable media device and then attaching the password to it.'[17]

23. New and different challenges to data handling arise from innovations in communication technology through access-based controls to electronic records, greater use of email, and the opportunity to store large amounts of data in relatively small devices. Furthermore, the cultural and behavioural aspects of the management of patients' information should not be overlooked. The recent review of data sharing undertaken by Richard Thomas and Mark Walport recommended 'a significant improvement in the personal and organisational culture of those who collect, manage and share personal data'.[18].

[17] Information Commissioner, 2009. ICO issues stark reminder to NHS bodies on patient records, 30 April 2009. Available at: http://www.ico.gov.uk/upload/documents/pressreleases/2009/nhs_trusts_undertakings_280409.pdf [accessed 3 July 2009]

[18] Thomas R, Walport M. 2009 Data Sharing Review Report. Available at: http://www.justice.gov.uk/reviews/datasharing-intro.htm [accessed 3 July 2090]

24. We have to remain alert to other challenges to the confidentiality and security of patients' information that may arise from beyond the healthcare sector. Emphasis in public policy for more widespread proactive sharing of personal data between different public services may lead to confusion among health professionals and others in healthcare about their obligations. It may also undermine the public's trust that their medical data is being held securely and confidentially for the purpose it was collected, and for which they gave their consent.

25. The GMC told us about research commissioned to examine public and professional attitudes to the privacy of healthcare data as part of their recent review of guidance on confidentiality. This report found that:
    - The public appears to be becoming more comfortable with computer technology, which may reduce fears over privacy, but with increasing expectations over security and choice about access to their records
    - Doctors seem poorly briefed on privacy issues
    - Not much research has been done with other professions despite their use of records in patient care
    - Professionals' concerns are centred on legal or regulatory uncertainties, gauging risks of internal and external threats to privacy, and assuring patients of their confidentiality.

    This review reflected on the changing context of healthcare records. Whereas historically their role was in ensuring treatment, continuity of care and providing some legal defence, the authors remarked that changing legislation and the introduction of new technologies marked a change that enabled and demanded greater sharing of information and wider thoughts about ownership of records.[19]

26. We should not expect every instance of professional practice to be covered in detail by the regulators' standards. This would be disproportionate. Regulators' standards and codes of conduct emphasise the responsibilities of professionals that should be adhered to in the course of practice. Employers' and organisations' policies echo these principles in guidance on their implementation in the context of practice.

27. However, we have to accept and anticipate changing views and expectations among the public about the confidentiality and security of their data, both in healthcare and more widely. The public profile of threats to personal data demands that regulators act promptly and take this issue seriously.

28. When regulators provide guidance to registrants it is essential that changes in the public's expectations around these issues are noted and reflected, as well as new legal requirements or challenges that emerge from innovative use of information technology. We were interested to learn that the GMC plan further work with doctors to promote their revised guidance on confidentiality. They will be exploring the possibility of developing practical tools such as screensavers for doctors to download that highlight the importance of locking computers and not sharing passwords.

29. In considering whether further action around codes of conduct is necessary, it would be helpful to be able to assess the current threats and risks to the security of personal medical data. These may arise from technical, systemic or behavioural issues.

---

[19] GMC, 2007. Public and Professional attitudes to privacy of healthcare data: a survey of the literature. Available at: http://www.gmc-uk.org/guidance/news_consultation/GMC_Privacy_Attitudes_Final_Report_with_Addendum.pdf [accessed 29 June 2009]

However, it is hard to draw conclusions based on regulators' experience; the number of cases considered by FTP panels is relatively small and cases represent a particular set of circumstances. Furthermore, regulators can only take action when in receipt of a complaint and data misuse issues may be dealt with locally by employers.

30. The commission asks whether the definition of misconduct should be changed to incorporate the responsibilities of different parties with respect to electronic data. We use 'misconduct' as a general reference to indicate impaired fitness to practise as it is not a term consistently defined in all regulatory bodies' legislation. That being so, and given the principle-based, context-neutral nature of regulators' standards, redefining the term 'misconduct' would not, in our view, be an appropriate or necessary course of action.

31. None the less, electronic data can introduce new threats in practice which may be involved in complaints about fitness to practise. Thinking about individual cases, a challenge may arise in ensuring that changing social expectations and awareness of emerging threats from technical innovation are appreciated by FTP panellists. Through our reviews of the outcomes of FTP cases CHRE offers feedback and learning points to regulators to help promote excellence in regulation and we have expressed concern when issues around personal data appear to have been taken lightly.

Conclusion

32. Data misuse in healthcare is a challenge, not least because of changing individual and social expectations around personal data generally and in healthcare. New methods of storing and accessing data present novel threats both in terms of the scale of potential losses and in the opportunity for misuse. We would expect regulators and other agencies to take the rapid developments in this area seriously and respond in a timely way. At the same time, the risks to patient confidentiality posed by the design of healthcare settings, permitting confidential discussions to be overheard, for example on hospital wards, in reception areas and in lifts, cannot be overlooked.

33. The principles embedded in regulators' codes and standards about confidentiality and security of patients' information are timeless and neutral in terms of practice settings. The standards themselves are satisfactory in their current form. However, their application by health professionals and regulators is contemporary and has to respond to changes in the wider environment to ensure data is not misused. We welcome additional guidance from regulators to support professionals' practice. This should be available in a timely fashion to enable registrants to meet patients' needs and expectations, especially when circumstances change. Where misconduct may arise, assessments of complaints about fitness to practise should reflect the wider circumstances of the allegations, and we believe this should include consideration of the public's current expectations of professionals' handling of their personal data and a clear appreciation of the new threats that emerge from developments in technology.

34. The health professional regulators are one part of the framework guiding professionals' use of patients' data. The regulators' role and responsibility in influencing the conduct of health professionals is complemented by the work of other agencies, notably employers, commissioners, other regulators and governments. Ultimately the prevention of data misuse is a joint effort across these organisations.

The actions that regulators can take to prevent data misuse or to apply sanctions in cases of misconduct are one element of this endeavour.

Appendix 1: Data misuse
Relevant extracts from regulators' core standards and codes of conduct

General Chiropractic Council - *Code of Practice and Standard of Proficiency*

A2. Chiropractors must keep information about patients confidential.[20]

Specifically chiropractors:

A2.1. must take the appropriate precautions when communicating confidential or sensitive information electronically, in writing or orally. Such precautions should take account of: who might overhear or oversee the information; who might access the information; the information that might be communicated by the practitioner's actions.

A2.2. must not disclose information about a patient, including the identity of the patient, either during or after the lifetime of the patient without the consent of the patient or the patient's legal representative.[21]

A2.3. must store information in, and retrieve it from, recording systems consistent with the requirements of legislation relating to information and its use. Specifically chiropractors should ensure that when they use electronic recording systems, the records are safe from access outside the practice, the security and integrity of data is maintained and the system is safely backed-up at regular intervals.

A2.4. must maintain patient confidentiality during the handling, storage and disposal of records.

A2.5. must obtain consent from patients before responding to any requests for information about them. The chiropractor must also explain to the patient the chiropractor's own responsibilities in the process.

A2.6. must take all reasonable steps to ensure that others who work for or with them also maintain confidentiality.

A2.7. may make exceptions to the general rule of confidentiality and disclose information to a third party if:

- the chiropractor believes it to be in the patient's best interest to disclose information to another health professional or relevant agency
- the chiropractor believes that disclosure to someone other than another health professional is essential for the sake of the patient's health[22]
- disclosure is required by statute
- the chiropractor is directed to disclose the information by any official having a legal power to order disclosure, or
- having sought appropriate advice, the chiropractor is advised that disclosure should be made in the public interest.[23]

---

[20] Legislation relating to information and its use includes: the Data Protection Act 1998. "This Act provides a framework that governs the processing of information that identifies living individuals – personal data. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope eg it also covers personnel records". Department of Health, July 2003, *Confidentiality: NHS Code of Practice,* DH, London. This document contains other information likely to be of interest to chiropractors.

[21] This requirement has specific implications in a number of ways for chiropractors. Firstly, chiropractors should make sure that if they employ a bookkeeper or an accountant then financial information on payments can be looked at separately from clinical records. Secondly, if a chiropractor wishes to pursue a patient for overdue payments, then only the minimum information for the situation in hand should be supplied to outside bodies (eg for legal proceedings or for debt collection). Thirdly, for chiropractors thinking of selling their business there is a need to gain the patients'

[22] See section **E2.7** for further guidance on child protection.

[23] Public interest means those "exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services." (Department of Health, 1993, *Confidentiality: NHS Code of Practice*, DH, London).

In each case where disclosure is made by a chiropractor in accordance with an exception to the general rules of confidentiality a chiropractor must:

- as far as reasonably practicable, inform the patient before the disclosure take place[24]
- as far as reasonably practicable, make clear to the patient the extent of the information to be disclosed, the reason for the disclosure and the likely consequence of the disclosure, where it is appropriate to do this
- record in writing the reasons for the disclosure and to whom it was it was made
- record in writing the information disclosed and the justification for such disclosure
- where the patient is not informed before the disclosure takes place, record in writing the reasons why it was not reasonably practicable to do so
- disclose only such information as is relevant ensuring that the person to whom the disclosure is made undertakes to hold the information on the same terms as those to which the chiropractor is subject.

General Dental Council - *Standards for Dental Professionals*

3. Protect the confidentiality of patients' information

3.1. Treat information about patients as confidential and only use it for the purposes for which it is given.

3.2. Prevent information from being accidentally revealed and prevent unauthorised access by keeping information secure at all times.

3.3. In exceptional circumstances, it may be justified to make confidential patient information known without consent if it is in the public interest or the patient's interest. You should get appropriate advice before revealing information on this basis. Follow our guidance 'Principles of patient confidentiality'.

General Medical Council - *Good Medical Practice*

37. Patients have a right to expect that information about them will be held in confidence by their doctors. You must treat information about patients as confidential, including after a patient has died. If you are considering disclosing confidential information without a patient's consent, you must follow the guidance in with *Confidentiality: Protecting and providing information*.

Confidentiality: protecting and providing information

1. Patients have a right to expect that information about them will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care. If you are asked to provide information about patients you must:

- inform patients about the disclosure, or check that they have already received information about it;
- anonymise data where unidentifiable data will serve the purpose;

[24] "This will not be possible in certain circumstances, eg where the likelihood of a violent response is significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation." (Department of Health, 1993, *Confidentiality: NHS Code of Practice*, DH, London).

- be satisfied that patients know about disclosures necessary to provide their care, or for local clinical audit of that care, that they can object to these disclosures but have not done so;
- seek patients' express consent to disclosure of information, where identifiable data is needed for any purpose other than the provision of care or for clinical audit – save in the exceptional circumstances described in this booklet;
- keep disclosures to the minimum necessary; and
- keep up to date with and observe the requirements of statute and common law, including data protection legislation.

…
4. When you are responsible for personal information about patients you must make sure that it is effectively protected against improper disclosure at all times.

5. Many improper disclosures are unintentional. You should not discuss patients where you can be overheard or leave patients' records, either on paper or on screen, where they can be seen by other patients, unauthorised health care staff or the public. You should take all reasonable steps to ensure that your consultations with patients are private.

General Optical Council - *Code of conduct for individual registrants*
A registered optometrist or dispensing optician must:

3. respect patients' dignity and privacy;
…
6. maintain adequate patients' records;
…
12. respect and protect confidential information;

General Osteopathic Council - *Code of Practice*
As an osteopath, you must:
Maintain, respect and protect patient information, by

- taking full and accurate case histories
- maintaining full and accurate clinical records
- keeping patient information confidential
- keeping all patient records secure.

…

104. Patients have a right to expect that you will observe the rules of confidentiality. Unless you do so, patients will be reluctant to give you the information you need to provide good care.

105. In normal circumstances, you should keep confidential your patients' identities and other personal information you learn and record, along with the opinions you form in the course of your professional work. This duty extends to your staff and survives the death of any patient.

106. Similarly, you should not release or discuss the personal information, medical details or care of a patient with their partner or family members unless you have the patient's consent to do so.

107. You must ensure that the confidential information for which you are responsible is at all times secure against loss, theft and improper disclosure.

108. You may release confidential information if a patient, or someone appointed on their behalf, gives you specific permission to disclose it. It may not always be necessary to disclose all the information you hold on a patient. When seeking a patient's consent to disclose information about them, you must make sure they understand the extent of what you will be disclosing, the reasons for doing so and the likely consequences.

109. You must explain to patients the circumstances in which information about them is likely to be disclosed to others in your workplace and involved in their healthcare. Allow them to withhold permission for this if they wish. You must advise healthcare workers to whom you disclose information that they must also respect the patient's confidentiality.

…
120. Any patient records that you keep are subject to the provisions of the Data Protection Act 1998. If you retain personal information on individuals, you must register with the Information Commissioner.

Health Professions Council - *The standards of conduct, performance and ethics*
2. You must respect the confidentiality of service users.
You must treat information about service users as confidential and use it only for the purposes they have provided it for. You must not knowingly release any personal or confidential information to anyone who is not entitled to it, and you should check that people who ask for information are entitled to it.
You must only use information about a service user:
- to continue to care for that person; or
- for purposes where that person has given you specific permission to use the information.

You must also keep to the conditions of any relevant data protection laws and always follow best practice for handling confidential information. Best practice is likely to change over time, and you must stay up to date.

…
10. You must keep accurate records.
Making and keeping records is an essential part of care and you must keep records for everyone you treat or who asks for your advice or services. You must complete all records promptly. If you are using paper-based records, they must be clearly written and easy to read, and you should write, sign and date all entries.
You have a duty to make sure, as far as possible, that records completed by students under your supervision are clearly written, accurate and appropriate.
Whenever you review records, you should update them and include a record of any arrangements you have made for the continuing care of the service user.
You must protect information in records from being lost, damaged, accessed by someone without appropriate authority, or tampered with. If you update a record, you must not delete information that was previously there, or make that information difficult to read. Instead, you must mark it in some way (for example, by drawing a line through the old information).

Nursing and Midwifery Council - *The Code: Standards of conduct, performance and ethics for nurses and midwives*
Respect people's confidentiality
- You must respect people's right to confidentiality
- You must ensure people are informed about how and why information is shared by those who will be providing their care
- You must disclose information if you believe someone may be at risk of harm, in line with the law of the country in which you are practicing

Keep clear and accurate records
- You must keep clear and accurate records of the discussions you have, the assessments you make, the treatment and medicines you give and how effective these have been
- You must complete records as soon as possible after an event has occurred
- You must not tamper with original records in any way
- You must ensure any entries you make in someone's paper records are clearly and legibly signed, dated and timed
- You must ensure any entries you make in someone's electronic records are clearly attributable to you
- You must ensure all records are kept confidentially and securely

Pharmaceutical Society of Northern Ireland - *Code of Ethics*
Principle 2:
Respect and protect confidential information
Obligations:
2.1 Respect the confidentiality of information, professional or otherwise, acquired in the course of professional practice and only use it for the purposes for which it is given and in compliance with current legislation.
2.2 Maintain systems which ensure security of information and prevent unauthorised access to it.
2.3 Ensure that all who have access to patient/client information know and respect its confidential nature.
2.4 Ensure that confidential information is not disclosed without consent, except where legally permitted or in exceptional circumstances.

Royal Pharmaceutical Society of Great Britain – *Code of Ethics*
The Code of Ethics sets out seven principles of ethical practice that you must follow as a pharmacist or pharmacy technician. It is your responsibility to apply the principles to your daily work, using your professional judgement in light of the principles.

3.5 Respect and protect the dignity and privacy of others. Take all reasonable steps to prevent accidental disclosure or unauthorised access to confidential information and ensure that you do not disclose confidential information without consent, apart from where permitted to do so by the law or in exceptional circumstances.

3.6 Obtain consent for the professional services, treatment or care you provide and the patient information you use.

3.7 Use information obtained in the course of professional practice only for the purposes for which it was given or where otherwise lawful.

6.6 Comply with legal requirements, mandatory professional standards and accepted best practice guidance.