FSRH The Faculty of Sexual & Reproductive Healthcare

Service Standards for Confidentiality in Sexual and Reproductive Health Services

2020 | FSRH

The Faculty of Sexual and Reproductive Healthcare (FSRH) is the largest UK professional membership organisation working in the field of sexual and reproductive health (SRH). We support healthcare professionals to deliver high quality healthcare, including access to contraception. We provide our 15,000 doctor and nurse members with National Institute for Clinical Effectiveness (NICE) accredited evidence-based clinical guidance, including the UKMEC, the gold standard in safe contraceptive prescription, as well as clinical and service standards.

The FSRH provides a range of qualifications and training courses in SRH, and we oversee the Community Sexual and Reproductive Healthcare (CSRH) Specialty Training Programme to train consultant leaders in this field. We deliver SRH focused conferences and events, provide members with clinical advice and publish *BMJ Sexual & Reproductive Health* – a leading international journal. As a Faculty of the Royal College of Obstetricians and Gynaecologists (RCOG) in the UK, we work in close partnership with the College but are independently governed.

The FSRH provides an important voice for UK SRH professionals. We believe it is a human right for women and men to have access to the full range of contraceptive methods and SRH services throughout their lives. To help to achieve this we also work to influence policy and public opinion working with national and local governments, politicians, commissioners, policy makers, the media and patient groups. Our goal is to promote and maintain high standards of professional practice in SRH to realise our vision of holistic SRH care for all.

www.fsrh.org

Published by the Clinical Standards Committee

Faculty of Sexual and Reproductive Healthcare
of the Royal College of Obstetricians and Gynaecologists

First Published: 2015
Review date: 2020
Next review date: 2023

Contents

SERVICE STANDARDS FOR CONFIDENTIALITY IN SEXUAL AND REPRODUCTIVE HEALTH SERVICES

Changes Introduced since Review

- Implementation of Data Protection Act 2018
- End-of-document references replaced by footnotes
- Updated guidance on identity theft

Introduction

Information is held under legal and ethical obligations of confidentiality. Service users entrust their healthcare providers with sensitive and confidential information with the legitimate expectation that staff will respect this trust. All employees are responsible for maintaining and protecting this information.[1] All identifiable information, whether written, computerised, visually or audio recorded, or held in the memory of health professionals, is subject to the duty of confidentiality.[2] This is of particular importance in matters relating to sexual and reproductive health, and services must keep up to date with current national policies and guidance.

The Care Quality Commission (CQC) has published guidance (website updated Feb 2019) for their regulated organisations, following the introduction of the Data Protection Act 2018 and incorporating the National Data Guardian's standards with advice on meeting the requirements of the new legislation.[3] The key principles of the relevant legislation are summarised in Appendix A.

[1] NHS England, 2019. *Confidentiality Policy.*
[2] British Medical Association, n.d. *Confidentiality and Health Records Tool Kit.*
[3] Care Quality Commission, 2016. *Code of Practice on Confidential Personal Information.*

1 Standard Statement on Confidentiality Policies

All services should have a written Confidentiality Policy.

Service confidentiality policies should be informed by, and updated in line with, latest national guidance, e.g. from the Department of Health,[4, 5, 6, 7, 8, 9, 10, 11] General Medical Council, and other professional organisations.[5, 6]

1.1 Service confidentiality policies should be in line with and endorsed by local NHS Trusts.

1.2 All staff should sign up to the service's confidentiality policy.

1.3 Policies should include guidance on:

1.3.1 Handling written, electronic and verbal or audio information[12, 13]

1.3.2 Staff to whom the policy applies

1.3.3 Sharing information with other NHS services, and non-NHS organisations and agencies in line with current guidance [1, 13, 17]

1.3.4 Young people[7, 8, 20, 14, 15, 16]

1.3.5 Those unable to give consent[44, 5, 7]

1.3.6 Avoidance of inadvertent breach of confidentiality[5, 8, 12]

---

[4] NHS Scotland, 2012. *Protecting Patient Confidentiality.*
General Medical Council, 2007. *DH, GMC, and IC Issue Joint Guidance on Patient Data*.
Nursing and Midwifery Council, 2008. *The Code: Standards of Conduct, Performance and Ethics for Nurses and Midwives.*
Association of Medical Secretaries, Practice Managers, Administrators and Receptionists. *AMSPAR's Code of Conduct.*
[5] British Medical Association, n.d. *Confidentiality and Health Records Tool Kit.*
[6] Faculty of Sexual and Reproductive Healthcare, 2016. *Service Standards for Sexual and Reproductive Healthcare.*
[7] General Medical Council, 2017. *Confidentiality: Good Practice in Handling Patient Information.*
[8] Royal College of General Practitioners Adolescent Primary Care Society, 2009. *The Confidentiality and Young People Toolkit.*
[9] The Caldicott Committee, 1997. *Report on the Review of Patient-Identifiable Information*.
[10] Department of Health, 2010. *Confidentiality: NHS Code of Practice – Supplementary Guidance.*
[11] National Data Guardian for Health and Care, 2016. *Review of Data Security, Consent and Opt-Outs.*
[12] Department of Health, 2003. *Confidentiality: NHS Code of Practice*.
[13] Department of Health, 2016. *Records Management: Code of Practice for Health and Social Care.*
[14] Department of Health, 2011. *Quality Criteria for Young People Friendly Health Services.*
[15] Department for Children, Schools and Families, 2010. *Working Together to Safeguard Children.*
[16] Faculty of Sexual and Reproductive Healthcare, 2019. *FSRH Clinical Guideline: Contraceptive Choices for Young People.*

1.3.7 Disposal of confidential information[5, 13]

1.3.8 Legal and professional framework around confidentiality[44, 12, 17, 18, 19, 20]

1.3.9 Secure storage of paper and electronic records[9], visual and audio recordings, and of email, faxes, and SMS[5, 13, 21]

1.3.10 Patient access to paper and electronic records[22, 19]

1.3.11 Copying letters to patients [13, 23]

1.3.12 Safeguarding children[5, 7, 15]

1.3.13 Safe transporting and storage of patient records (both paper-based and electronic) when it is necessary to take them in cars or keep at home, e.g. for domiciliary visits[24]

1.3.14 Procedure for reporting incidents involving breaches of security or confidentiality

1.3.15 Procedures for use of CCTV and recording of telephone calls, publication in print, radio, TV, video, and internet media[5]

1.3.16 Disclosure required by statute; disclosure to police, social services and partner organisations; disclosure to solicitors, courts, tribunals and regulatory bodies; disclosure for insurance and occupational health purposes and financial audit; statutory restrictions on disclosure, and disclosure in public interests[5]

1.3.17 Procedures for secondary uses of information[5] such as research, epidemiology, public health surveillance, health service planning, and education

1.3.18 Procedures for handling patient information for teaching and training, including logbooks, training portfolios, and electronic staff records

1.3.19 Procedures for seeking advice in circumstances when staff are uncertain whether a disclosure without consent is justified

1.3.20 Information Governance training for staff

1.3.21 How the implementation of the policy will be monitored, reviewed and compliance assessed

1.4 Service users should be involved in the production and implementation of the service's confidentiality policy.

1.5 The processing of personal data must satisfy the requirements of data protection law, which imposes duties on data controllers. This guidance aims to be consistent with data protection law.

---

[17] Public Health England, 2009. *HIV and STI: Data Sharing Policy.*
[18] UK Caldicott Guardian Council, 2017. *A Manual for Caldicott Guardians.*
[19] HM Government, 1990. *Access to Health Records Act 1990*.
HM Government, 1991. *Age of Legal Capacity (Scotland) Act 1991.*
Department of Health and Social Care, n.d. *Personal Information Charter.*
[20] Department of Health, 2004. *Best Practice Guidance for Doctors and other Health Professionals on*

the Provision of Advice and Treatment to Young People under 16 on Contraception, Sexual and Reproductive Health.

[21] NHS, 2016. *Guidelines on Use of Encryption to Protect Person Identifiable and Sensitive Information.*

[22] Khong, S., Currie, I. & Eccles, S., 2008. *NHS Connecting for Health and THE National Programme for Information Technology.* The Obstetrician & Gynaecologist.

[23] General Medical Council, 2013. *Communication Partnership and Teamwork.*

[24] NHS Business Services Authority, 2018. *Home Working Computer Security Policy*.

2 Standard Statement on Confidentiality Training

All patients have the right to expect that information about them will be held in confidence. Patients must be properly informed as to how identifiable information about them is used.

2.1 All staff should receive training in confidentiality on taking up employment within the NHS or under contract to an NHS organisation and this training should be regularly updated in line with local Trust policies.[5]

2.2 Clinical and non-clinical personnel should receive accessible and appropriate training in confidentiality and handling enquiries about sensitive information, including proxy access.[12, 8, 25]

2.3 All staff should receive Caldicott training.[44, 18]

2.4 All staff should be trained in the legal requirements of the Data Protection Act[44, 19, 26] and the Freedom of Information Act 2000[27] as they apply to health services.

2.5 All staff should receive training on national Safeguarding Children procedures,[15] and be able to use local Safeguarding Children policies.

2.6 All staff should receive information security training. This should include training on the secure use of personally identifiable information in both paper and electronic record systems, including fax machines, electronic mail, and all forms of portable computing media such as laptops, handhelds, and USB memory sticks.[12, 25]

2.7 Training must be supported by ensuring that staff have ready access to organisational policies, procedures, and guidance documents, and know where to go for advice when needed.[5]

[25] Department of Health, n.d. *Information Governance Toolkit.*
[26] NHS England, 2018. *NHS Information Governance - Guidance on Legal and Professional Obligations*.
[27] HM Government, 2000. *Freedom of Information Act 2000.*

3 Standard Statement on Patients' Rights to Confidentiality

All services should prominently display their confidentiality statement, which should acknowledge that information will be shared with colleagues within the service in order to provide quality and continuity of care, except in certain well-defined circumstances.

3.1 All patients have the right to expect that information about them will be held in confidence. Patients must be properly informed as to how identifiable information about them is used.

3.2 Specific permission should be sought from the patient regarding the communication to them of test results and any other information, i.e. whether writing, telephoning, texting or any other means is acceptable to them.

3.3 There should be a mechanism for returning undelivered patient letters without opening them or breeching patient confidentiality, e.g. PO Box number.

3.4 Explicit consent should be sought for the use or disclosure of personal health information, unless it is clearly implied.[4, 5, 7] Specific permission should be sought from the patient to sharing any information with anyone outside the service, other than those directly involved in patient care. Information disclosed for secondary uses such as audit, service planning, medical research etc. should be anonymised or pseudonymised, but if this is not practicable, the patient's express consent should be sought.[5]

3.5 When patients withhold consent to disclosure of their information, their wishes should be respected.[5, 7]

3.6 With issues relating to safeguarding children, the patient should be informed that sharing will occur and the reasons for the disclosure should be given.[5, 15] There may be an exception to this when telling a victim of abuse that information will be shared may alert the abuser who could move elsewhere and cease harm to others.

3.7 All staff should be familiar with guidance about the use of photographs and video recordings.[5, 28]

3.8 No personally identifiable or sensitive information held in electronic format should be transferred across the NHS or to another organisation unless encrypted[21]. The transfer of clinical information or other personally identifiable information to other professionals by encrypted email.

[28] Department of Health, 2009. *Reference Guide to Consent for Examination or Treatment: Second Edition.*

3.9 All patient records, paper and electronic, should be securely stored and only be accessed on a “need to know / see” basis.[29]

3.10 The transfer of written clinical information to other professionals by letter, email or fax should be secure, and clearly marked “In Confidence”.

3.11 The Caldicott principles[9, 10] should be applied to all information sharing concerning patients.

[29] Department of Health and Social Care, 2007. *Information Security Management: NHS Code of Practice.*

4 Standard Statement on Disclosure without Consent

Services should display information for patients explaining that personal information can be disclosed if required by law or in public interests.

4.1 Confidentiality is an important duty, but it is not absolute.[1, 5, 7, 10, 15] The General Medical Council (GMC) has produced guidance on patient confidentiality and potential situations in which disclosure may be appropriate.[30] These include disclosures required by law, those made for the protection of patients and others, such as involvement in serious crime or child sexual exploitation or disclosure for health protection.[31] The "Confidentiality: Key legislation" factsheet can be used to healthcare professionals in their decision making[32] (see Appendix B for full description of applicable legislation).

4.2 All staff should be made aware that if they are in any doubt about whether to share information, they should seek advice from an experienced colleague, the safeguarding lead, a Caldicott Guardian, a regulatory body or defence organisation. Decisions should be made in conjunction with appropriate others wherever possible.

4.3 Disclosure without consent can be justified in the public interest to enable medical research if that research is approved by a Research Ethics Committee. Staff should alert Research Ethics Committees to disclosures of identifiable information without consent when applying for approval for research projects.[4]

4.4 All staff must document in the patient's record their reasons for disclosing information without consent and any steps they have taken to seek the patient's consent, to inform them about the disclosure, or their reasons for not doing so.

4.5 Services should have safeguards in place to deal with medical identity theft, including knowledge of the reporting mechanisms should it be identified. Suspected or actual medical identity theft can be reported at https://cfa.nhs.uk/reportfraud.[33]

[30] General Medical Council, 2017. *Disclosures for the Protection of Patients and Others.*
[31] Public Health Executive, 2014. *Notifications of Infectious Diseases (NOIDS).*
[32] General Medical Council, n.d. *Confidentiality: Key Legislation*.
[33] Office of Inspector General, n.d. *Medical Identity Theft.*

5 Standard Statement on Working with Young People

Services should ensure that all staff have received adequate training in confidentiality as it applies to patients, including situations where confidentiality may be lawfully breached.

5.1 All staff should familiarise themselves with guidance from Department of Health,[43, 18] NICE[34] and the GMC[35] on the care of young people accessing sexual health services.

5.2 All staff working with young people should be familiar with, and use, Fraser Guidelines[4, 16] (or appropriate equivalent guidance) on assessing competence.

5.3 All staff working with young people should be aware of local and national safeguarding children/child protection guidance and procedures and their impact on confidentiality.[1, 2, 15]

5.4 Services should use the self-review tool to ensure they meet the criteria outlined in the Department of Health's "You're Welcome: Quality criteria for young people friendly health services",[14] or the "Pregnancy and Parenthood Young People Strategy" if based in Scotland.[36]

5.5 All staff working with young people in primary care settings should consider if proxy access arrangements to their GP records requires amendment.[37]

[34] National Institute for Health and Care Excellence, 2007. *Sexually Transmitted Infections and Under-18 Conceptions: Prevention Public Health Guideline [PH3].*
[35] General Medical Council, 2018. *0-18 Years: Guidance for All Doctors.*
[36] NHS Scotland, 2016. *Outcomes Framework and Supporting Evidence for the Pregnancy and Parenthood in Young People Strategy in Scotland*.
[37] Royal College of General Practitioners, 2015. *Online services: Proxy Access on behalf of Children and Young People Guidance for General Practice*

6 Standard Statement on Sharing Non-identifiable Information

Services should ensure that information is freely available to patients, informing them that anonymised information may be used for service improvement, audit, and clinical governance purposes.

6.1 Information used for clinical governance, audit, teaching or other quality improvement purposes should always be anonymised or pseudonymised.[38]

6.2 Clinical services information should contain a statement concerning the use of anonymised information, including explanation about information from screening programmes and disease registers, applicable to the setting and system in which the healthcare provider works. [1, 18, 39]

6.3 As health informatics and genomics services develop enhanced capabilities, including the reliable linkage of patient data, relevant guidance should be referred to where available.[40]

[38]NHS Business Services Authority, 2015. *Pseudonymisation and anonymisation of Data Policy.*
[39] Department of Health, Social Services and Public Safety, 2012. *Code of Practice on Protecting the Confidentiality of Service User Information.*
[40] NHS Health Informatics Service, n.d. *Information Governance.*

7 Standard Statement on Disposal of Confidential Information

All services should have effective mechanisms for the disposal of confidential information.

7.1 Services should follow national guidelines for archiving and disposing old notes.[19]

7.2 All staff should have easy access to shredding for all paper carrying identifiable information (including notes on message pads).

7.3 Identifiable audio or electronic information should be collected and stored in accordance with current GMC Guidelines.[41]

7.4 Paper records transferred to electronic systems must be stored in accordance with the latest iteration of guidance appropriate for the storage method.[42]

[41] General Medical Council, 2011. *Storing and Disposing of Recordings.*
[42] Faculty of Sexual and Reproductive Healthcare, 2019. *Service Standards for Record Keeping.*

Appendix A

Legal Standards

There are three areas of law that are particularly relevant to the processing of confidential information. These are:

1. Human Rights Act 1998

Article 8 of the Human Rights Act establishes a right to 'respect for private and family life, home and correspondence'.[4] This right is not absolute, but anyone who processes patient information must do so in accordance with the law. This may include disclosure in the interests of security, public safety, or for the protection of health.

2. Data Protection Act 2018

The Data Protection Act 2018 incorporates the European General Data Processing Regulation (GDPR) and regulates the processing of personal data.[44]

All organisations that collect and use personal data must comply with these regulations and in doing so must:

- Process the least possible amount of personal data
- Only keep it for as long as necessary
- Carry out assessments to make sure personal data is processed in a lawful way
- Protect data and identify risks to privacy
- Consider if the person needs to give their consent for collection of their data
- Understand and respect the rights of the person whose data is being is collected
- Appoint a data protection officer
- Be transparent and open about the processing of personal data
- Report any security breaches

3. The Common Law of Confidentiality

Common law is built up from case law, where practice has been established by individual judgements, and is based on binding precedents set following other cases. The key principle is that information confided for the purpose of receiving care and treatment should not be processed for other purposes except in circumstances where the law permits or requires it.

Circumstances which may make disclosure of confidential information lawful include:

- Where the individual to whom the information relates has capacity and has given

[43] HM Government, 1998. Human Rights Act 1998.
[44] HM Government, 2018. Data Protection Act 2018.

valid consent

- Where disclosure is necessary to safeguard the individual or others, or is in the public interest
- Where there is a legal duty to do so, for example a court order

Appendix B[45]

Disclosure required by statute

Health professionals are required by law to disclose certain information, regardless of patient consent. Health professionals must be aware of their obligations to disclose in these circumstances as well as to ensure that they do not disclose more information than is necessary. Where such a statutory requirement exists, patients' consent to disclosure is not necessary. Patients have no right to refuse but they should be generally aware of the disclosure and that it is to a secure authority.

Examples of statutory disclosures include:

- Public Health (Control of Disease) Act 1984 and Public Health (Infectious Diseases) Regulations 1988 - a health professional must notify local authorities of the identity, sex and address of any person suspected of having a notifiable disease, including food poisoning
- Abortion Regulations 1991 - a doctor carrying out a termination of pregnancy must notify the Chief Medical Officer, giving a reference number and the date of birth and postcode of the woman concerned
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985 - deaths, major injuries, and accidents resulting in more than three days off work, certain diseases, and dangerous occurrences must be reported
- Road Traffic Act 1988 - health professionals must provide to the police, on request, any information which may identify a driver alleged to have committed a traffic offence
- Terrorism Act 2000 - all citizens, including health professionals, must inform police as soon as possible of any information that may help to prevent an act of terrorism, or help in apprehending or prosecuting a terrorist
- The Information Sharing Index (England) Regulations 2007 (ContactPoint) - health professionals must provide basic identifying information to the local authority for every child up to the age of 18.

Disclosure to the police, social services and partner organisations

Some statutes permit, rather than require, disclosure. Examples include the Data Protection Act 1998, the Crime and Disorder Act 1998 and the Children Act 1989, which permit disclosure to other organisations, such as the police, local authorities, social services, schools, Multi-Agency Protection Panels and government bodies.

In such cases, health professionals may only disclose information when the patient has given consent or there is an overriding public interest. If health professionals have any doubts about

[45] General Medical Council, 2017. *Confidentiality: Good Practice in Handling Patient Information.*

whether the disclosure is a statutory obligation, they should ask the person or body applying for the information to specify under which legislation it is sought.

Disclosure to solicitors

Health records that are required for legal proceedings are usually obtained via the Data Protection Act 1998 or Access to Health Records Act 1990. Health professionals releasing information to lawyers acting for their patients should ensure that they have the patient's written consent to disclosure and, where there is any doubt, confirm that the patient understands the nature and extent of the information disclosed.

In practice, most solicitors will provide the patient's signed consent when requesting confidential information. If a solicitor acting for someone else seeks information about a patient, their consent to the release of the information must be obtained. Should the patient refuse, the solicitor may apply for a court order requiring disclosure of the information.

Disclosure to courts, tribunals, and regulatory bodies

The courts, including the coroner's courts, some tribunals, and bodies appointed to hold inquiries such as the General Medical Council, have legal powers to require disclosure, without the patient's consent, of information that may be relevant to matters within their jurisdiction. Applications for court orders must be served on patients who, if they object to the disclosure of the information, must be given an opportunity to make representations to the court. However, often applications are served on healthcare organisations when they should be served on patients. In these circumstances the patient should be informed of the application so they can make their representations to court if they object.

Where a court order is served, health professionals are justified in disclosing information when they believe on reasonable grounds that information falls within this category, and should disclose only as much information as is requested. Failure to comply with a court order to release records may be an offence, but health professionals should object to the judge or presiding officer if they believe that the records contain information that should not be disclosed, for example, because it relates to third parties unconnected with the proceedings. Patients should be informed of disclosures ordered by a court.

Statutory restrictions on disclosure

Health professionals are required by law to restrict the disclosure of some specific types of information.

For example:

- The Gender Recognition Act 2004 allows trans people who have taken decisive steps to live fully and permanently in their acquired gender to apply for legal recognition of that gender. The Act makes it an offence to disclose 'protected information' when that information is acquired in an official capacity. It defines 'protected information' as information about a person's application to the Gender Recognition Panel for gender recognition and a person's gender history after that person has changed gender under the Act. At the time of writing, Department of Health guidance for healthcare professionals regarding the Act, and specifically how this type of patient information

should be recorded, stored and shared is awaited.

- The NHS (Venereal Diseases) Regulations 1974 (currently being reviewed by the Department of Health) and the NHS Trusts and PCTs (Sexually Transmitted Diseases) Directions 2000 provide that any information capable of identifying an individual who is examined or treated for any sexually transmitted disease including HIV shall not be disclosed, other than to a medical practitioner in connection with the treatment of the individual or for the prevention of the spread of the disease.
- The Human Fertilisation and Embryology Act 1990 protects the confidentiality of the information kept by clinics and the Human Fertilisation and Embryology Authority (HFEA). Information can only be viewed by the clinic licence-holder and by staff or members of the HFEA (plus, in certain circumstances, the Registrar General or a court). Disclosure of information which identifies the patient to another party without the patient's prior consent is a criminal offence.