Confidentiality Policy

Introduction

Practitioners and clinics will use a vast array of internal policies and procedures, but the most appropriate policies will always depend on the size and nature of the individual organisation. The policies are more effective if they are developed and reviewed on an ongoing basis with the involvement of staff and are tailored to suit the specific needs of a clinic and its activities. However, some guidance and examples mean that you don't have to start from scratch.

Save Face has developed a number of example generic policies which can be used as a basis for your own policies, where relevant these policies should be tailored to suit the needs and requirements of each individual practitioner and clinic.

Disclaimer

Save Face accepts no responsibility for any third-party loss or consequences arising from the use of these example policies.

Confidentiality; Guidance Notes and Background Information

This policy should be read in conjunction with Managing Medical Records Policy and Privacy policy (GDPR)

A duty of confidentiality arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. This duty of confidence is derived from:

- Common law – the decisions of the Courts
- Statute law which is passed by Parliament

Legislation

All staff must be aware of the following legislation and understand their responsibilities relating to confidentiality:

The General Data Protection Regulations 2018

This Act governs the processing of information that identifies living individuals. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and electronic.

The Mental Capacity Act (2005)

This provides a legal framework to empower and protect people who may lack capacity to make some decisions for themselves. The assessor of an "individual's capacity to make a decision will usually be the person who is directly concerned with the individual at the time the decision needs to be made" this means that different health care workers will be involved in different capacity decisions at different times.

The Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002

These Acts grant people rights of access to information that is not covered by the Data Protection Act 1998, e.g. information which does not contain a person's identifiable details.

The Computer Misuse Act 1990

This Act secures computer programs and data against unauthorized access or alteration. Authorized users have permission to use certain programs and data. If the users go beyond what is permitted, this is a criminal offence.

Disclosure

Disclosure means the giving of information. Disclosure is only lawful and ethical if the individual has given consent to the information being passed on. Such consent must be freely and fully given. Consent to disclosure of confidential information may be:

- Explicit
- Implied
- Required by law or

- Capable of justification by reason of the public interest

Disclosure with Consent

Patients have a right to access their own medical records and receive copies of them, subject to certain safeguards. Administration fees cannot be charged.

Explicit consent is obtained when the person in the care of a clinician agrees to disclosure having been informed of the reason for that disclosure and with whom the information may or will be shared. Explicit consent can be written or spoken. Implied consent is obtained when it is assumed that the person understands that their information may be shared within the clinical team. Clinicians should make the people in their care aware of this routine sharing of information, and clearly record any objections.

Disclosure without Consent

The term ‘public interest’ describes the exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader social concern. Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others. Each case must be judged on its merits. These decisions are complex and must take account of both the public interest in ensuring confidentiality against the public interest in disclosure. Disclosures should be proportionate and limited to relevant details.

Clinicians should be aware that it may be necessary to justify disclosures to the courts or to the appropriate statutory regulator and must keep a clear record of the decision making process and advice sought. Courts tend to require disclosure in the public interest where the information concerns misconduct, illegality and gross immorality.

Disclosure to Third Parties

This is where information is shared with other people and/or organizations not directly involved in a person’s care. Clinicians must ensure that the people in their care are aware that information about them may be disclosed to third parties involved in their care. Patients generally have a right to object to the use and disclosure of confidential information. They need to be made aware of this right and understand its implications. Information that can identify individual people in the care of a healthcare professional must not be used or disclosed for purposes other than healthcare without the individual's’ explicit consent, some other legal basis, or where there is a wider public interest.

Confidentiality after Death

The Police and Criminal Evidence Act (1984)

The duty of confidentiality does continue after death of an individual to whom that duty is owed.

Information Disclosure to the Police

In English law there is no obligation placed upon any citizen to answer questions put to them by the police. However, there are some exceptional situations in which disclosure is required by statute.

Police Access to Medical Records

The police have no automatic right to demand access to a person's medical records. Usually, before the police may examine a person's records they must obtain a warrant under the Police and Criminal Evidence Act 1984. Before a police constable can gain access to a hospital, for example, in order to search for information such as medical records or samples of human tissue, he or she must apply to a circuit judge for a warrant. The police have no duty to inform the person whose confidential information is sought, but must inform the person holding that information.

This Act allows healthcare professionals to pass on information to the police if they believe that someone may be seriously harmed or death may occur if the police are not informed. Before any disclosure is made healthcare professionals should always discuss the matter fully with other professional colleagues and, if appropriate consult their statutory regulator or professional body or trade union. It is important that healthcare professionals are aware of their organizational policies and how to implement them. Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. If disclosure takes place without the person's consent they should be told of the decision to disclose and a clear record of the discussion and decision should be made as stated above.

Special Considerations to be Taken into Account when Disclosure is Being Considered

In some circumstances it may not be appropriate to inform the person of the decision to disclose, for example, due to the threat of a violent response. The clinician may feel that, because of specific concerns, a supplementary record is required containing details of the disclosure. The GDPR 2018 does allow for healthcare professionals to restrict access to information they hold on a person in their care, if that information is likely to cause serious harm to the individual or another person. A supplementary record should only be made in exceptional circumstances as it limits the access of the person to information held about them. All members of the healthcare team should be aware that there is a supplementary record and this should not compromise the persons' confidentiality.

Acting as a Witness in a Court Case

If summoned as a witness in a court case he/she must give evidence. There is no special rule to entitle healthcare professionals to refuse to testify. If the individual refuses to disclose any information in response to any question put to him/her, then a judge may find the individual in contempt of court and may ultimately send him/her to prison.

Risk or Breach of Confidentiality

If a member of staff identifies a risk or breach of confidentiality they must raise their concerns with someone in authority if they are unable to take affirmative action to correct the problem and record that they have done so. A risk or breach of confidentiality may be due to individual behavior or as a result of organizational systems or procedures.

Confidentiality is a fundamental part of professional practice that protects human rights. This is identified in Article 8 (Right to respect for private and family life) of the European Convention of Human Rights which states:

The common law of confidentiality reflects that people have a right to expect that information provided is only used for the purpose for which it was given and will not be disclosed without permission. This covers situations where information is disclosed directly and also to information obtained from others. One aspect of privacy is that individuals have the right to control access to their own personal health information.

- All staff will respect people's right to confidentiality.
- Staff must ensure people are informed about how and why information is shared by those who will be providing their care as per privacy policy.
- Staff must disclose information if they believe someone may be at risk of harm, in line with the law of the country in which you are practicing.

'The General Data Protection Regulation 2018 requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence.'

The fee for registration is £35 per annum. Further details and registration forms can be found on http://ico.org.uk/

References and Further Reading

- Patient Confidentiality (GDC)
- Standards for Dental Professionals (GDC,2013)
- Confidentiality (GMC)
- The Code: Standards of conduct, performance and ethics for nurses and midwives (NMC, 2018)
- The General Data Protection Regulations 2018 (GDPR)
- European Convention on Human Rights Act (2000)
- The Computer Misuse Act 1990
- The Freedom of Information Act 2000
- The Freedom of Information (Scotland) Act 2002
- The Mental Capacity Act (2005)

Template Confidentiality Policy

Policy Statement

Facial Sculpting Limited is committed to providing a confidential service to its users. No information given to Facial Sculpting Limited will be shared with any other organisation or individual without the user's explicit consent.

For the purpose of this policy, confidentiality relates to the sharing of personal, sensitive or identifiable information about individuals or organizations (confidential information), which comes into the possession of the organisation through its work.

Facial Sculpting Limited holds personal data about its staff, users, members etc. which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organisation without prior permission.

All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

Purpose

The purpose of the Confidentiality Policy is to ensure that all staff, members and users understand the organization's requirements in relation to the disclosure of personal data and confidential information.

Principles

- All personal paper-based and electronic data must be stored in accordance with the GDPR 2018 and must be secured against unauthorized access, accidental disclosure, loss or destruction.
- All personal paper-based and electronic data must only be accessible to those individuals authorized to have access.
- Facial Sculpting Limited is committed to effective audit of the use of and quality of its services in order to monitor performance. All audit records shared with third parties, such as to support staff appraisal or monitoring reports for regulators shall be produced in anonymous form, so individuals cannot be recognised.

Protecting Confidentiality in Discussions

It is not acceptable for staff to:

- Discuss matters related to the people in their care outside the clinical setting
- Discuss a case with colleagues in public where they may be overheard
- Discuss one patient with another without explicit and written consent.
- Consultations must not be undertaken where privacy and confidentiality cannot be assured.

Protecting Confidentiality Using the Telephone

- If telephone conversations to patients or potential patients are conducted in areas where they may be overheard, such as in reception or waiting areas, staff will not verbalize any identifiable confidential information, such as names, addresses or telephone numbers.
- Answer phone messages must not be played back aloud, where they can be overheard
- Messages, if confidentiality may be breached, must not be left on answer phones without the express permission of the patient.

Protecting confidentiality Using Computers/ internet

- Computer screens should not be visible to members of the public
- Access to data held on a computer must be password protected with access restricted to personnel with permissions
- Confidential patient information should not be shared by email without encryption

Protecting Confidentiality patient records (see policy- medical records)

Protecting confidentiality using social media or mobile devices

- Practitioners/employees will avoid using mobile devices to communicate with patients where confidential sensitive information might be disclosed.
- Respect all communication by text or messenger apps as part of the medical record.
- Practitioners will not store or retain patient information on mobile devices.
- Where mobile devices are used, devices must be password protected and stored securely.
- All confidential information must be stored securely on a cloud (not on the device itself) and encrypted.
- Explicit and written consent must be obtained for sharing any patient information, including photographs, on social media.

Records

All hard copy records are kept in locked filing cabinets. All digital records are maintained securely in compliance with GDPR 2018. All hard copy information relating to service users will be kept securely. This includes notebooks, copies of correspondence and any other sources of information.

Breaches of Confidentiality

Facial Sculpting Limited recognizes that occasions may arise where individual workers feel they need to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged where there is risk of danger to the individual, a volunteer or employee, or the public at large, or where it is against the law to withhold it. In these circumstances, information may be divulged to external agencies e.g. police or social services on a need to know basis.

Legislative Framework

Facial Sculpting Limited will monitor this policy to ensure it meets statutory and legal requirements including the GDPR 2018. Training on the policy will include these aspects.

Ensuring the Effectiveness of the Policy

All staff members will receive a copy of the confidentiality policy, and associated guidance notes. Existing and new workers will be introduced to the confidentiality policy via induction and training. The policy will be reviewed annually and amendments will be proposed and agreed by the director Germana Bal. Staff members are required and supported to develop and maintain an understanding of information governance appropriate to their role.

Non-Adherence

Breaches of this policy will be dealt with under the Grievance and/or Disciplinary procedures as appropriate.