Confidentiality Policy

Document Control

Confidentiality Notice

Document Details

Organisation:	Derma
Current Version Number:	1
Current Document Approved By:	Rima Clayton
Date Approved:	22/07/2020
Next Review Date:	22/07/2022

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments

Confidentiality Policy

INTRODUCTION

The reasons for the policy:

- All information about the organisation (in particular user data) is confidential, whether held electronically or in hard copy
- Other information about Derma (for example its financial matters) is confidential
- Staff will of necessity have access to such confidential information from time to time.
- 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.

RELEVANT CQC FUNDAMENTAL STANDARD/H+SC ACT REGULATION (2014)

- Regulation 10: “Dignity and Respect”.

APPLICABILITY

The policy applies to all employees and contractors engaged by Derma (collectively referred to herein as ‘members of staff’).

POLICY

- Members of staff must not under any circumstances disclose service user information to anyone outside Derma except to other health professionals on a need-to-know basis, or where the user has provided written consent, or for some other legal reason (e.g. Court Order regarding disclosure).

- All information about users is confidential: from the most sensitive diagnosis, to the fact of having visited the clinic or being registered with the organisation.

- Members of staff must not under any circumstances disclose other confidential information about the company to anyone outside Derma unless with the express consent of the CQC Registered Manager or representative.

- Members of staff should limit any discussion about confidential information only to those who need to know within Derma.

- The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.

- All patients can expect that their personal information will not be disclosed without their permission (except in the most exceptional circumstances when disclosure is required when somebody is at grave risk of serious harm).

- Electronic transfer of any confidential information must be encrypted. Members of staff must take particular care that confidential information is not transmitted in error by email or over the Internet.

- Members of staff must not take data from the organisation's computer systems (e.g. on a memory stick or removable drive) off the premises unless authorised to do so.

- Members of staff who suspect a breach of confidentiality must inform the CQC Registered Manager or representative immediately.

- Any breach of confidentiality will be considered as a serious disciplinary offence and may lead to dismissal.

- Members of staff remain bound by the requirement to keep information confidential even if they are no longer employed at Derma.

- Any breach, or suspected breach, of confidentiality after the worker has left Derma's employment will be passed to the organisation's lawyers for action.

- Any patient wishing to have access to their own records will be treated in accordance with statutory requirements.

RESPONSIBILITIES OF MEMBERS OF STAFF

All health professionals must follow their professional codes of practice and the law. This means that they must make every effort to protect confidentiality. It also means that no identifiable information about a user is passed to anyone or any agency without the express permission of that user, except when this is essential for providing care or necessary to protect somebody's health, safety or well-being.

All health and social care professionals are individually accountable for their own actions. They should, however, also work together as a team to ensure that standards of confidentiality are upheld, and that improper disclosures are avoided.

Additionally, the organisation:

- is responsible for ensuring that everybody employed or engaged by Derma understands the need for, and maintains, confidentiality.
- has overall responsibility for ensuring that systems and mechanisms are in place to protect confidentiality.

Standards of confidentiality apply to all staff who are bound by contracts of employment, contracts for service or other forms of engagement to maintain confidentiality. They must not reveal to anybody outside the organisation, personal information they learn in the course of their work, or due to their presence in the surgery, without the user's consent. Nor will they discuss with colleagues any aspect of a user's attendance at the surgery in a way that might allow identification of the user unless to do so is necessary for the user's care. These requirements will be conveyed to all staff as part of their induction when first joining the organisation.

GENERAL PRINCIPLES

The general principle to remember is that nothing is to be revealed to an enquirer. The identity of callers must be established and, if necessary, return calls made to confirm this.

Personal visits from either the police or press should be handled with courtesy. Following confirmation of their identity, they should then be referred to the CQC Registered Manager or deputy.

Any clinical details or personal information contained within the user's medical records must not be discussed with friends or relatives. This includes confirming a user has attended the clinic for whatever reason. A user's reason to attend the clinic may be something they do not wish to discuss with their family, or require others to know about.

It is important to note that individual users are not identified for purposes of training or any other activity.

IF DISCLOSURE TO THIRD PARTIES IS NECESSARY

If a user or another person is at grave risk of serious harm which disclosure to an appropriate person would prevent, the relevant health professional should take advice from the CQC Registered Manager or representative, and/or from a professional / regulatory / defence body, in order to decide whether disclosure without consent is justified to protect the user or another person. If a decision is taken to disclose, the user should always be informed before disclosure is made, unless to do so could be dangerous.

Any decision to disclose information to protect the health, safety or well-being of an individual will be based on the degree of current or potential harm, not the age of the user.

In addition, there may be instances where disclosure is necessitated by reason of legal process (e.g. Court Order). In addition, on occasions the Police may approach Derma for information about a user e.g. in case of serious crime. Such situations will call for careful judgement, and will normally need to be subject to confirmation by a Director. Medical staff involved will also be well advised to consult their professional indemnity organisation in advance of any disclosure.

<u>Information relating to a user may be disclosed for the following reasons</u>:

- Information relating to a user may be disclosed provided the user has given his/her written authorisation for his/her legal representative to obtain it.
- Where a user has died, consent to release information should be sought from the Executor of the estate.
- Where the user has died intestate, consent to release information should be sought from the next of kin.
- When healthcare professionals involved with the users' care require to share clinical information in the strictest confidence.
- When adverse drug reactions may be reported by any authorised professional staff to the Committee on Safety of Medicines.

<u>Release of Information as a Legal Requirement</u>

- Certain infectious diseases must be notified under the Public Health (Infectious Disease) Regulations 1968. Failure to comply is a criminal offence (Infection Control Office).

- If a user is suspected of addiction to a scheduled drug, a doctor is required to inform the Chief Medical Officer of the Home Office Drugs Branch (Misuse of Drugs Notification & Supply to Addicts Regulation 1985).
- The Road Traffic Act 1972 requires information to be given to the police, which may lead to the identification of the driver of a vehicle. Only the name and address may be given.
- Any individual must give information to the police which may prevent an act of terrorism or lead to the apprehension of a person involved in such an act (The Prevention of Terrorism (Temporary Provisions) Act 1989).
- A professional member of staff's duty of confidentiality may be overridden when failure to disclose information would expose the user, or someone else, to the risk of death or serious harm. Where a professionally qualified person feels unable to disclose, the police or Crown Prosecution Service may apply for a Court Order under the Police & Criminal Evidence Act 1984.
- In the event of sudden, suspicious or unexplained deaths, the Coroner may wish to investigate. Information should be disclosed, to determine whether an inquest should be held.
- Any person must obey a written legal order to attend court and produce confidential evidence.
- Identifiable information, relating to users being treated for sexually transmitted diseases, shall not be disclosed, except for the purpose of treatment or prevention.
- If a healthcare professional has reason to suspect child abuse, it is legitimate to supply information to appropriate authorities, to ensure the safety of the child is maintained.
- Access to computer held information under the Data Protection Acts.

.

CONFIDENTIALITY GUIDELINES FOR MEMBERS OF STAFF

- Be aware that careless talk can lead to a breach of confidentiality – discuss your work only with authorised personnel, preferably in private.
- Always keep confidential documents away from prying eyes.
- Verbal reporting about users should be carried out in private. If this is not possible, it should be delivered in a volume such that it can only be heard by those for whom it is intended.
- When asking for confidential information in circumstances where the conversation can be overheard by others, conduct the interview in as quiet and discreet a manner as possible and preferably find somewhere private for the discussion.
- Information should be given over the telephone only to the user or, in the case of children, to their parent or guardian. Precautions should be taken to prevent the conversation being overheard. Care must be taken to ensure that the duty of confidentiality to a minor is not breached, even to a parent.

- The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.
- When using computers, unauthorised access should be prevented by password protection and physical security such as locking the doors when offices are left unattended. Where possible, VDU screens should be positioned so that they are visible only to the user. Unwanted paper records should be disposed of safely by shredding on site and computer files on hard or floppy disks should be wiped clean when no longer required.
- If unsure about authorisation to disclose, or a person's authorisation to receive confidential information, always seek authorisation from the CQC Registered Manager or representative before disclosing any personal health information.

DECLARATION BY MEMBERS OF STAFF

The following declaration or equivalent should be signed by all relevant members of staff at Derma e.g. as part of their contract of employment/Contract for Service, or otherwise as appropriate:

I understand that all information about users held by Derma is strictly confidential, including the fact of a particular user having visited the organisation.

I will abide by the confidentiality guidelines and principles set out in the organisation's Confidentiality Policy.

I have read the Staff Confidentiality Policy above and fully understand my obligations and the consequences of any breach of confidentiality. I understand that a breach of these obligations may result in dismissal.

I understand that any breach, or suspected breach of confidentiality by me after I have left Derma employment will be passed to the Company's lawyers for action.

If I hold a professional qualification and my right to practise depends on that qualification being registered with a governing body, it is my responsibility to have read and understood their advice on confidentiality.

Name: _____ *Signature:* _____
Date: _____

LEGISLATION

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

The Data Protection Act 1998

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

This Act grants 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 unauthorised access or alteration. Authorised users have permission to use certain programmes 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

Explicit consent is obtained when the person in the care of a professional staff 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. Professional staff 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 into account of both the public interest in ensuring confidentiality against the public interest in disclosure. Disclosures should be proportionate and limited to relevant details.

Professional staff 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 organisations not directly involved in a person’s care. Professional staffs must ensure that the people in their care are aware that information about them may be disclosed to third parties involved in their care. Users 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 nurse, doctor or dentist 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 duty of confidentiality continues after the 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 organisational 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 professional staff may feel that, because of specific concerns, a supplementary record is required containing details of the disclosure. The Data Protection Act 1998 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 behaviour or as a result of organisational 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.
- 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 Data Protection Act 1998 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. Further details and registration forms can be found on: http://ico.org.uk/