Compliance Plan

Pursuant to the General Data Protection Regulation (GDPR), our data compliance plan is set out below.

The three individuals with access to personal data are the medical secretary (hereafter MedSec), data protection officer (hereafter DPO), and the Consultant (referred to together as the Principals). The office (hereafter the Office) consists of the computer systems on which data is stored, in addition to the physical copies of patient notes.

As data controllers, the company does not process data beyond storage except for the following reasons:

- Contacting insurers and debt collectors regarding invoices
- Contacting General Practitioners, other consultants, and hospitals regarding patient details (such as for upcoming surgeries).

In the latter case, patients may opt out, as per GDPR stipulations.

Records of data stored are stored in the office on the premises, to which only the Principals have access.

Following a brief data flow audit, this compliance plan was written in order to provide information for the ICO, companies and individuals with which the Office deals, and patients who may request information on our data protection policy.

For any questions regarding this data compliance plan or Cosmetic Associates Limited broader GDPR documentation, the Principals can be contacted via email (plasticsurgery@ramakrishnan.co.uk).

Data storage

- **In physical form**:
    - Patient files dating back to 1995 are kept in a secure location on the premises, behind a locked door. Access to these files are only available to the MedSec, DPO, and the Consultant.
- **Data retention**
    - After consideration, the Principals concluded that 30 years was a suitable data retention period, in line with other independent hospitals and health care providers
    - This length of storage reflects the fact that whilst some details (such as addresses) may change over time, it is useful for both the Consultant and the patients to have a history of the surgery for follow-up procedures or general awareness. If patients request this information to be deleted, the Principals can comply by shredding the physical files and deleting the electronic copies (following 'Deleting personal data' Version 1.1 from the Information Commissioner's Office).
    - More details about the data retention policy can be found on our website, Cosmetic Surgery Essex.

- **In digital form:**
    - All digital data is stored on three computers in the Office, behind a locked door to which only three parties discussed above have access.
    - Data transfers within the office use a server, which is secured and password protected. A secure iCloud account, as instituted by YellowSpring (the IT services provider of the Office) is used for maintaining images.
    - Patient records are generated via Private Practice Manager (hereafter PPM). PPM has confirmed its
    - The secure email service Egress is used to contact other consultants, hospitals, and patients, allowing for encrypted transfers of personal data.

Personal Information

- The following types of personal information are contained in the physical and digital files:
        - Names
        - Occupations
        - Medical procedures
        - Addresses
        - Contact information
        - Photographs (pre- and post-operative)
        - Date of birth
        - Medical history
        - Race and gender
- The data is collected from patients' General Practitioners (GPs), consultants, hospitals, and from patients themselves.

Data sharing

- Data is only shared with the following companies or individuals, for the purposes of providing health care.
- All of the following companies or individuals have completed GDPR compliance, as signified by contracts provided to us and available to the ICO:
    - Health sector:
        - Hospitals
        - General Practitioners
        - Consultant surgeons
        - Private Practice Manager (PPM) software
        - Medical Secretaries
    - Financial sector:
        - Healthcode
        - Providers Online
        - Debt collectors
        - Accountant
    - IT services:
        - YellowSpring
- Details of the specifics of data sharing can be found in GDPR compliance contracts prepared by each of these companies or individuals, and which can be provided on request.

Communications

- Egress is a secure emailing application which allows for transferring both emails and files securely between users. This allows for transfers of larger files as well as emails to important third party contractors such as hospitals and general practitioners, which is necessary for the provision of health services.
- Egress was chosen as it is used by several hospitals with which the Consultant is working, making it easy to use the encrypted features when sending files to them. However, as the ICO itself acknowledges, these features are complex for members of the public (in this case, patients) to use. As such, we will be offering patients a choice of either encrypted emails through Egress (with links to the application and an explanation of why we are using this service), or of continuing to use Microsoft Outlook with a warning that it not a fully encrypted service.

Storage of computers and related equipment

- As the computers in the Office contain sensitive personal information, a number of security features are used to ensure privacy. First and foremost, they are password protected, with a new password updated every two weeks using a random password generator. Secondly, the Office uses Windows 7, a supported operating system, with plans to move to Windows 10 or later when updates stop. The system is regularly updated with security patches in order to avoid any security issues.
- The Consultant uses a digital camera in order to produce photographs of patients, as is necessary in order to provide health care. The camera is transported to and from hospital in a locked container and carried in a locked bag as is necessary. All photographs pertaining to patients are stored on the computers in the Office weekly, before being deleted from the camera.
- The Consultant's laptop is carried to and from hospital in a locked container or is otherwise stored in the Office. It is password protected and security updated. Hard drives, pen drives, and an iPad containing photographs are stored in the Office and are similarly protected.
- The Consultant's National Health Service (NHS) office also contains hard drives with photographs. These are securely stored in a locked office.

Training

- All three Prinicpals have completed relevant Data Protection Awareness Training so as to understand both the importance of the GDPR and ways in which to best ensure data protection by design is enacted.
- Training has been provided by the Spire Healthcare group (in person), and through the Nuffield Health group (in a webinar). Both also are familiar with the ICO website and its

Grounds for information processing

- Consent is the legal basis for processing patient's data. In response to GDPR, the Principals have produced a patient-consultant contract, which explicitly explains patients' rights, and comes with in opt-in by choice, unticked box to show consent has been understood and is

given. This is also accessible at Cosmetic Surgery Essex, where it is regularly updated in order to take into account any changes of import.

- Following Article 9 (2) (h) of the GDPR, special category data is required for the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.
- No children are processed, and thus provisions related to data processing of minors are not relevant.
- No automated decision making is used in the Office, and as such, these provisions of the GDPR are not applicable

Erasure

- Data stored on computers can be deleted entirely (i.e. erased in such a state that it cannot be reconstituted).
- Data stored in files can be shredded so as to make it essentially impossible to reconstruct.