DEFINITIONS

Personal Data – means information concerning an individual who can be identified whether directly or indirectly.

Data Subject means a named or otherwise identifiable individual who is the subject of personal data.

Data Concerning Health means personal data related to the physical or mental health of an individual which reveals information about his or her health status. The law defines "Genetic data" and "Special Category Data" separately.

Data Processing means any use whatsoever of personal data. This includes collection, organization, storage, alteration, combining, retrieval, consultation, disclosure, restriction, erasure or destruction of personal data. All processing of personal data requires a legal basis.

Data Processor means an entity that processes personal data on behalf of, and on the instruction of, the data controller. Example- a contract with a laboratory or software service provider. It is any person other than an employee of the data controller, who possesses the data on behalf of the data controller.

Data Controller means the individual or party that determines how and why personal data is processed (that is, the purposes and means of processing). For doctors working in a public or private hospital, the hospital or regional authority is likely to be the data controller. The obligations under the DPA apply primarily to Data Controllers.

Joint or Co-Controller means two or more data controllers jointly determine the purposes and the means of the data processing to be carried out. This might be applicable to doctors in independent medical practices.

Data Controller Representative means a person or other entity appointed for the purpose.

Data Protection Standards means the standards set out in the Act §22-31: Personal data shall be processed:

1.**Fairly and lawfully** using consent.
2.Must be used for the specific stated purpose only.
3.**Adequate, relevant & limited to what is necessary for purpose**
4.Must be **accurate**
5.Shall not be kept longer than necessary
6. Consistent with the **rights of the data subject**
7. **Technical & Organizational measures in place**
8.Shall not be transferred to a State or authority outside of Jamaica unless under certain specified conditions.

Data Breach means a breach of security that has led to an accidental or unlawful disclosure, alteration, loss or destruction of personal data.

References:
Data Protection Act, 2020
General Data Protection Regulation & Medical Practice – RCPI, 2021
GMC - Introduction to data protection for Independent practitioners, March 7, 2022

DATA PROTECTION ACT

Provided as a courtesy

FOR MORE INFORMATION: Contact
Medical Association of Jamaica
19A Windsor Avenue, Kingston 5.
Tel: 876-946-1105
E: info@majdoctors.com

The Data Protection Act of 2020 will come into effect on the 1st of December, 2023 and gives significant operational obligations to the Data Controller to ensure that the data protection standards are met as well as giving obligation to report to the Office of the Commissioner for any breach under the Act.

Who is a Data Controller?

This is 'a person or public authority, who either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed only for purposes for which they are required under any enactment to be processed..'

A sole medical doctor in independent practice is, therefore, the Data Controller. Where more than one doctors use the medical practice, one other may be registered as Joint Data Controller. In large multiple sites medical practices it is important to give thought to who must be the designated Data Controller. Similarly as with private and public entities the practice manager or the CEO of the medical practice can be the designated Data Controller.

What are the obligations of the Data Controller?

The Data Controller is obliged to:

1. ensure that there are appropriate **technical and security measures** implemented within the medical practice.

2. devise **a Privacy Policy** to outline to patients how their information will be treated (posters, leaflets in the waiting room, web site etc).

3. develop **Record Processing Activities**

4. Formulate **Data Processing Contracts** with data service providers such as software, security companies and laboratories.

5. Ensure the level of **security measures** that are appropriate to the data breach risk.

6. Ensure a **Data Protection Officer** is engaged with the appropriate skills, expert knowledge of data protection law and have due regard to the level of risk to monitor internal compliance, ensure staff training, supports Data Protection Impact Assessment, advises on data protection obligation and acts as a contact point for data subjects and Data Controller

7. **implement security systems** which have regard to pseudonymisation, encryption, secure door access to restricted area, reviewing swipe care access every 6 months, changing key codes periodically, setting computers to lock automatically, prohibiting sharing of user accounts to access personal data, and securely locking filing cabinets used to store personal data etc.

8. **Notify the Commission of data breach**. Breaches that pose any risk to privacy must be reported to the commission within 72 hours of it coming to the attention of the Data Controller. Where there is a breach and there are no implementable measures to eliminate the risk, the patient must be promptly informed. Medical practices, therefore, must have a written protocol on how to manage personal data breaches and ensure all staff are trained accordingly.

How should the Data Controller discharge his/her duties?

The Data Controller should do an audit of the medical practice to understand how patient data are collected, stored, retrieved and secured and thus identify the gaps with respect to the requirements of the Data Protection law. You should identify your lawful basis for processing personal data.

Formulate the necessary policies to make the medical practice compliant (Privacy, security, health records administrative procedures including accessing, storing, retrieving and sharing).

Engage a Data Protection Officer for medical practice.

Commence training sessions with staff to establish that they have the requisite knowledge and skill in data protection and patient privacy.

Register the medical practice with the Office of the Information Commission.

Conduct annual audits and ensure compliance.