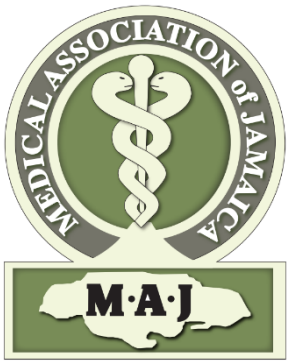
2023



Q & A Data Protection Act

WEBINAR JULY 25, 2023

BRIAN JAMES

1) Can organizations be recognized as data subjects?

No, organizations cannot be recognized as data subjects under the Data Protection Act. The term "data subject" refers to an identified or identifiable natural person to whom personal data relates. This means that the data subject is an individual, a human being, and not a legal entity such as an organization, company, or corporation. The rights provided by the Data Protection Act, such as the right to access personal data, the right to rectification, and the right to erasure, apply to individuals and not to organizations.

2) What are the rights of individuals under the Data Protection Act?

Under the Data Protection Act, individuals, also referred to as data subjects, have several rights regarding their personal data. These include:

1. Right to Access: Individuals have the right to be informed about the collection, use, storage, and disclosure of their personal data by a data controller. They can request access to their personal data and be given a description of the personal data, the purposes for which they are being processed, and the recipients or classes of recipients to whom they are or may be disclosed.
2. Right to Rectification: Individuals have the right to ask for the correction of incomplete or inaccurate personal data held by data controllers.
3. Right to Prevent Processing: Individuals have the right to request that a data controller not process or stop processing their personal data. They can require the data controller to cease or not to begin processing their personal data.
4. Right to Automated Decision Making: Individuals have the right to require that decisions which significantly affect them are not based solely on the automatic processing of their personal data.
5. Right to Data Portability: Individuals have the right to request that personal data that they provided to one data controller be transmitted to another data controller of their choice.
6. Right to Compensation: If an individual suffers distress or damage due to a contravention of the Act by a data controller, they are entitled to compensation.

These rights are subject to certain exemptions as set out in the Act. For example, access to personal data may be denied if it would compromise the confidentiality of the exempt data.

3) What are the exemptions to the rights of individuals under the Data Protection Act?

Under the Data Protection Act, there are several exemptions to the rights of individuals. These exemptions are often necessary for the protection of certain interests, such as national security, law enforcement, and public health. Here are some of the key exemptions:

1. National Security: Personal data may be exempt from the provisions of the Act if it is necessary for the purpose of safeguarding national security.
2. Law Enforcement: Personal data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty are exempt from certain provisions of the Act.
3. Public Health: Personal data processed for the purposes of protecting public health are exempt from certain provisions of the Act.
4. Research Purposes: Personal data processed only for research purposes are exempt from certain provisions if the results of the research or any resulting statistics are not made available in a form which identifies the data subjects.
5. Judicial Proceedings: Personal data necessary for the purpose of or in connection with any order or judgment of a court are exempt from certain provisions of the Act.
6. Parliamentary Privilege: Personal data are exempt from certain provisions if the exemption is required for the purpose of avoiding an infringement of the privileges of either House of Parliament.
7. Domestic Purposes: Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs are exempt from the data protection standards and the provisions of Parts II and III.
8. These exemptions are subject to certain conditions and limitations as set out in the Act. For more specific information, it is recommended to consult the relevant authorities or a legal expert.

4) Please clarify the ideal qualification for Data Protection Officers:

The ideal qualifications for a Data Protection Officer (DPO) as per the Jamaican Data Protection Act include:

1. The DPO should be an appropriately qualified person. While the Act does not specify the exact qualifications, it is generally understood that the DPO should have a deep understanding of data protection laws and practices.
2. The DPO should be capable of monitoring the data controller's compliance with the provisions of the Act in an independent manner. This means that there should not be any conflict of interest between the DPO's duties and any other duties that person might have.
3. The DPO should be able to consult with the Commissioner to resolve any doubts about how the provisions of the Act and any regulations made under the Act are to be applied.
4. The DPO should be able to ensure that the data controller processes personal data in compliance with the data protection standards and in compliance with the Act and good practice.
5. The DPO should have expertise in areas such as information communication technology, data protection or privacy rights, or other like skills.
6. The DPO should be a person of integrity, capable of exercising competence, diligence, sound judgment, and impartiality.
7. The DPO should be involved in all matters relating to the protection of personal data and should be provided with the necessary resources to perform his duties.
8. The DPO does not necessarily have to be an internal appointment - it can be an outsourced or shared service. However, the DPO's role is to monitor and advise on compliance and not to make decisions about the processing of data as that would conflict with the role.

Please note that these are general guidelines, and the exact qualifications may vary depending on the specific requirements of the organization and the nature of the data being processed.

5) Can a medical practitioner be his/her own data protection officer for a small private practice?

Yes, a medical practitioner can be their own Data Protection Officer (DPO) for a small private practice. However, there are certain conditions that need to be met. According to the Data Protection Act, the DPO should be an appropriately qualified person capable of monitoring the data controller's compliance with the provisions of the Act in an independent manner. This means that there should not be any conflict of interest between the DPO's duties and any other duties that person might have.

The DPO should also have expertise in areas such as information communication technology, data protection or privacy rights, or other like skills. They should be a person of integrity, capable of exercising competence, diligence, sound judgment, and impartiality.

However, it's important to note that the DPO's role is to monitor and advise on compliance and not to make decisions about the processing of data as that would conflict with the role. Therefore, it can be very difficult to identify someone who can be independent of processing decisions to fill this role, especially in a small practice where the medical practitioner is also the data controller.

6) Are data processors required to obtain consent from the data subject on the data to be collected?

No, data processors are not required to obtain consent from the data subject on the data to be collected. The responsibility of obtaining consent lies with the data controller. The data controller is the entity that determines the purposes and means of the processing of personal data. They are responsible for ensuring that the processing is based on one of the lawful bases set out in the Data Protection Act, which includes obtaining the data subject's consent.

However, the data processor, who processes personal data on behalf of the data controller, must comply with the instructions of the data controller and ensure appropriate security measures are in place. They must also assist the controller in complying with data subjects' rights, including reporting any personal data breaches to the controller immediately.

It's important to note that any processing of personal data must be done in accordance with the principles of the Data Protection Act, which includes obtaining informed, specific, and freely given consent from the data subject where consent is the basis for processing.

7) With regards to data being transmitted from physician to physician, would signed consent for transmission by patients enable this to be done within the law?

Yes, signed consent from patients would generally enable the transmission of their data from one physician to another within the law. The consent must be freely given, specific, informed, and unambiguous. It's important that patients are informed about what their data will be used

for, who it will be shared with, and how long it will be kept. They should also be informed of their right to withdraw their consent at any time.

However, there may be other conditions or exceptions depending on the specific circumstances and the nature of the data being transmitted. For instance, in some cases, data may be shared without consent if it is necessary for medical purposes and is undertaken by a healthcare professional or a person who owes a duty of confidentiality equivalent to that of a healthcare professional.

Please note that these are general guidelines, and the exact requirements may vary depending on the specific laws and regulations applicable in your jurisdiction. For more specific advice, please contact our lead expert Chukwuemeka Cameron.

8) When a patient requests a file, who pays for the copy, the doctor or the patient?

When a patient requests a copy of their personal data, the data controller may charge a reasonable fee based on administrative costs for any further copies requested by the data subject. This means that the patient would typically bear the cost for the copy. However, the exact procedures and costs may vary depending on the specific policies of the healthcare provider or the relevant regulations in place.

9) How does the act deal with health insurance payments. Is the data controller responsibility under the purview of the doctor or the insurance company?

The Data Protection Act (DPA) does not specifically address health insurance payments. However, it does provide guidelines on how personal data, including health data, should be handled.

In the context of health insurance payments, both the doctor and the insurance company could potentially act as data controllers, depending on the specific circumstances.

A data controller is defined as any 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.

In the case of a doctor, they could be a data controller if they are collecting and processing personal data (such as medical records) for the purpose of providing medical care.

On the other hand, an insurance company could be a data controller if they are collecting and processing personal data (such as medical records and payment information) for the purpose of providing insurance coverage and processing claims.

Both the doctor and the insurance company, as data controllers, would be responsible for ensuring that the personal data they process is handled in accordance with the provisions of the DPA. This includes implementing appropriate technical and organizational measures to protect the data, adhering to data protection policies, and registering with the relevant supervisory authority.

However, the exact responsibilities of the doctor and the insurance company would depend on the specific circumstances and the nature of the data being processed. For more specific advice, please contact our lead expert Chukwuemeka Cameron.

10) What determines which Data Controller or entity needs to appoint a Data Protection Officer?

The determination of which Data Controller or entity needs to appoint a Data Protection Officer (DPO) is outlined in the Data Protection Act. According to the Act, a data controller falls within the requirement to appoint a DPO if the data controller:

1. Is a public authority.
2. Processes or intends to process sensitive personal data or data relating to criminal convictions.
3. Processes personal data on a large scale.
4. Falls within a class prescribed by the Commissioner by notice published in the Gazette as being a class of data controllers to whom the requirement to appoint a DPO applies.

It's important to note that all public authorities are required to appoint a DPO. Furthermore, even if an organization does not fall within these categories, it is still recommended to have a data protection lead or a point of contact for data protection matters.

11) Should patients be given their file if they request it?

Yes, patients have the right to request their personal data, including their medical files, according to the principles of the Data Protection Act. This is often referred to as a Data Subject Access Request. The data controller, which could be a hospital or a clinic, is required to provide the requested personal data within a specified period, typically one month.

However, there may be certain exemptions or conditions, such as the presence of third-party data in the files, which may need to be redacted or removed. If the data is provided in an electronic format, it should be in a commonly used form based on the reasonable expectations of the data subject. It's also important to note that the data controller may charge a fee for providing further copies of the data based on administrative costs.

12) What are the exemptions or conditions for giving patients their files when they make requests for those files?

When patients make requests for their files, there are certain exemptions or conditions that may apply:

Identity Verification: The data user is not obliged to comply with a request for access to personal data unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the personal data which that person seeks.

Confidentiality: Compliance with the request is not required if it will be in contravention of any duty of confidentiality recognized by law.

Third Party Consent: If another person who can be identified from the personal data does not consent to the disclosure of his or her personal data to the person making the request, the data user is not obliged to comply with the request.

Exemptions: Compliance with the request is not required if it will be in contravention of the exemptions contained in Part IV of the Data Protection Act.

Special Needs: Special care should be taken to ensure that people with special needs can exercise their rights, for instance by proactively providing easily accessible elements to facilitate the exercise of these rights.

Third Party Data: If the data contains third party data, the data user must decide whether or not the third party data can be concealed. If this is not possible, the consent of the third party must be sought.

Please note that these are general guidelines and the exact conditions may vary depending on the specific requirements of the organization and the nature of the data being processed.

13) How is enforcement to be undertaken in relation to the Act? Will there be inspectors for example?

Enforcement under the Data Protection Act is primarily the responsibility of the Information Commissioner. The Commissioner has the duty to monitor compliance with the Act and any regulations made under the Act. The Commissioner also has the power to serve enforcement notices on data controllers who are found to be in contravention of the Act.

An enforcement notice will specify the provision of the Act that has been contravened and the action that the data controller is required to take to rectify the contravention. If the Commissioner considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the data protection standards, the Commissioner may cancel or vary the notice.

In addition to this, the Act provides for the issuance of warrants by a Magistrate, authorizing officers to enter premises for the purpose of discharging any functions or duties under the Act or Regulations. These officers, accompanied by members of the Police Force, may inspect and seize any documents or other material found on the premises that may constitute evidence of the commission of an offence under the Act.

The Act also provides for the right to appeal against an enforcement notice or the refusal of an application for cancellation or variation of the notice.

As for the question of inspectors, the documents do not explicitly mention the appointment of inspectors for the enforcement of the Act. However, the Commissioner's office is empowered to conduct audits and inquiries, and sanction for non-compliance.

14) In the case of the Regional Health Authorities (RHA) with responsibilities for several hospitals and health centres, does each health centre or hospital register as a Data Controller or should the RHA register on behalf of all the entities under its purview?

Based on the Data Protection Act, each entity that determines the purposes for which and the manner in which any personal data are, or are to be, processed is considered a Data Controller. Therefore, if each hospital and health centre under the Regional Health Authorities (RHA) independently determines the purpose and manner of data processing, they would each need to register as a Data Controller.

However, if the RHA is the entity that determines the purpose and manner of data processing for all the entities under its purview, then the RHA could register as the Data Controller on behalf of all these entities.

It's important to note that the specific circumstances and organizational structure of the RHA and its associated entities could influence this.

15) For communication via email, is data transmission (eg patient reports, summaries etc) via institutional email recommended?

Based on the information available, it is recommended that data transmission via institutional email should be done with caution, especially when it involves sensitive data such as patient reports or summaries. It is crucial to ensure that the email system is secure and that appropriate measures are in place to prevent unauthorized access or disclosure of personal data.

For instance, when sending emails that contain sensitive information, it is advisable to use secure methods such as encryption or pseudonymization. Additionally, the use of bulk email should be carefully managed to prevent accidental disclosure of data. For example, when sending bulk emails, the use of the BCC function is recommended to hide the recipients' email addresses from each other.

Furthermore, it is important to have policies and procedures in place regarding email use, and staff should receive adequate training on these policies. This includes understanding the risks associated with email communication and how to mitigate these risks.

However, it's important to note that the specifics may vary depending on the exact nature of the data being processed and the specific requirements of the organization.

16) Can you provide some examples of who would be best suited to be a Data Protection Officer? Is it that a solo medical practitioner CANNOT or in your opinion should not be the Data Protection Officer for his or her practice?

The Data Protection Officer (DPO) should ideally be a person with a deep understanding of data protection laws and practices and should have expertise in areas such as information communication technology, data protection or privacy rights, or other like skills. The DPO should be capable of monitoring the data controller's compliance with the provisions of the

Act in an independent manner, which means there should not be any conflict of interest between the DPO's duties and any other duties that person might have.

As for a solo medical practitioner acting as their own DPO, it's not explicitly prohibited by the Data Protection Act. However, it's important to consider the potential for a conflict of interest. The DPO's role is to monitor and advise on compliance and not to make decisions about the processing of data as that would conflict with the role. Therefore, if the solo medical practitioner is also making decisions about the processing of data, it could potentially create a conflict of interest.

In such cases, it might be advisable to outsource the DPO role to an expert for the first few years. During this period, a DPO in training can be identified and trained up with the appropriate certification and hands-on training.

Please note that these are general guidelines, and the exact qualifications may vary depending on the specific requirements of the organization and the nature of the data being processed.

17) For doctors who use Electronic Medical Records (EMR), if there is a data breach of the EMR, who is liable under the Act? Is it the doctor or the provider of the EMR service?

Under the Data Protection Act, both the data controller and the data processor have responsibilities to ensure the protection of personal data.

In the context of Electronic Medical Records (EMR), the doctor, who determines the purposes and means of processing personal data, is typically considered the data controller. The provider of the EMR service, who processes personal data on behalf of the data controller, is typically considered the data processor.

In the event of a data breach, the data controller (the doctor) is generally held responsible for any failure to comply with the requirements of the Act. This includes ensuring that the data processor (the EMR service provider) has taken appropriate technical and organisational measures to protect the data.

However, the data processor can also be held liable if they have not complied with the obligations of the Act that are specifically directed to processors or where they have acted outside or contrary to the lawful instructions of the data controller.

It's important to note that these are general principles and the specific circumstances of each case can influence where liability falls.

18) Radiologists see patients daily who require imaging under the EHCSD programme at several facilities. This requires that their images be compared between facilities. Is it recommended that a "Consent for Portability" is provided (following explanation) to facilitate the transfer of their images between platforms?

Based on the information available, it is recommended that a "Consent for Portability" is provided to facilitate the transfer of patient images between platforms. This consent should be informed, specific, and freely given by the patient. It is important to ensure that the patient fully understands what they are consenting to, including the nature of the data being transferred, the purpose of the transfer, and the entities that will have access to the data.

The consent should be documented in a manner that allows the patient to easily control what they have consented to and to withdraw their consent if they choose to do so. It is also crucial to ensure that the data transfer is conducted in a secure manner to protect the patient's privacy and confidentiality.

However, this is a general recommendation, and the specific requirements may vary depending on the local regulations and the specific circumstances of the case. For more specific advice, please contact our lead expert Chukwuemeka Cameron.

19) What is the proper action to be taken by a doctor who suspects that there is a data breach has occurred or is occurring while the patient data is under the control of an Electronic Medical Record provider?

If a doctor suspects that a data breach has occurred or is occurring while the patient data is under the control of an Electronic Medical Record provider, the following steps should be taken:

The doctor should immediately inform the data controller about the suspected breach. The data controller, in this case, could be the hospital, clinic, or healthcare organization that the doctor is affiliated with.

The data controller should then initiate an investigation to confirm whether a data breach has indeed occurred. This investigation should be prompt and thorough and should aim to establish if personal data have been compromised.

If the data breach is confirmed, the data controller is required to report the breach to the supervisory authority within 72 hours of becoming aware of it. This is in accordance with the Data Protection Act.

The data controller should also notify each data subject whose personal data is affected by the security breach. The notification should include the nature of the security breach, the

measures taken to mitigate the possible adverse effects of the breach, and the contact information of the data protection officer.

The data controller should take immediate steps to mitigate the effects of the breach and prevent further breaches. This could include measures such as resetting passwords, enhancing security protocols, and providing additional training to staff.

The data controller should document the breach, including its causes, effects, and the remedial action taken. This documentation will help the supervisory authority to verify compliance and may also help prevent future breaches.

Remember, these are general guidelines and the exact steps may vary depending on the specific circumstances of the breach and the policies of the data controller.

20) Does a Medical Report suffice as a copy of the patient file?

A medical report can be part of a patient's file, but it may not encompass the entire patient file. A patient's file typically includes a comprehensive record of all interactions, treatments, diagnoses, and medical procedures related to the patient. This can include medical reports, but also other elements such as test results, imaging studies, medication records, and notes from healthcare professionals. Therefore, while a medical report can provide important information about a patient's health status and medical history, it may not provide the complete picture that a full patient file would. It's also important to note that any sharing or handling of such files should be done in compliance with data protection laws to ensure the privacy and confidentiality of the patient's information.

21) Is there a distinction under the Act, between the file and the information contained therein? Does the patient own both or just the information?

Under the Data Protection Act, there is a distinction between the file and the information contained therein. The file is a system or method of storing and organizing data, while the information contained therein refers to the personal data of an individual.

The Act primarily concerns itself with the protection of personal data, which is defined as information relating to a living individual who can be identified from that information alone or from that information and other information in the possession of, or likely to come into the possession of, the data controller.

In terms of ownership, the Act does not explicitly state that the patient owns the information. However, it does provide individuals with certain rights over their personal data. These rights include the right to access their personal data, the right to correct inaccuracies in their

personal data, the right to object to the processing of their personal data, and the right to have their personal data erased in certain circumstances.

As for the file, it is typically owned by the entity that created it, such as a hospital or a doctor's office. However, the entity must comply with the provisions of the Act in terms of how they handle and process the personal data contained in the file.

For more specific information, I recommend reaching out to the relevant authorities or contacting our lead expert Chukwuemeka Cameron.

22) What are the consequences for data controllers who do not comply with the Data Protection Act?

Data controllers who do not comply with the Data Protection Act can face several consequences:

Monetary Penalties: Data controllers can be fined for contraventions of the Act. The amount of the fine can vary depending on the nature and severity of the contravention. For instance, a data controller can be liable upon summary conviction in a Parish Court to a fine not exceeding two million dollars or to imprisonment for a term not exceeding two years. In more severe cases, upon conviction on indictment in a Circuit Court, the fine can be higher, or imprisonment for a term not exceeding seven years.

Compensation Claims: If an individual suffers damage or distress due to a contravention of the Act by a data controller, the individual is entitled to seek compensation from the data controller.

Reputational Damage: Non-compliance with the Act can lead to reputational damage, which can subsequently lead to a loss of trust and potential business.

Enforcement Notices: The Commissioner can serve a data controller with a notice requiring them to comply with the data protection standards. Failure to comply with such a notice can result in further penalties.

Imprisonment: In some cases, contravention of the Act can lead to imprisonment.

It's important for data controllers to understand their obligations under the Act and to take steps to ensure compliance. Non-compliance can result in significant penalties and can harm the data controller's reputation.

23) Are there any exceptions to the consequences for data controllers who do not comply with the Act?

Yes, there are certain exceptions to the consequences for data controllers who do not comply with the Data Protection Act. These exceptions are often related to the nature of the contravention and the steps taken by the data controller to rectify the situation. Here are some key exceptions:

1. Due Diligence: If a data controller can prove that they exercised all due diligence to comply with the Act, this can serve as a defense in case of a contravention. The standard of proof in such cases is usually on the balance of probabilities.
2. Reconsideration and Rectification: If a data controller receives a notice of contravention, they are given a period to rectify the situation. If they take the necessary steps to comply with the Act within this period, they may avoid some of the consequences.
3. Compliance Measures: If a data controller takes all necessary measures to ensure full compliance with the provisions of the Act, especially the data protection standards, this can mitigate the consequences of non-compliance.
4. Reporting Contraventions: If a data controller reports any contravention of the data protection standards or any security breach affecting personal data to the Commissioner within seventy-two hours of becoming aware of it, this may influence the consequences they face.

However, these exceptions do not guarantee immunity from penalties and each case is usually assessed on its own merits. It's always recommended for data controllers to strive for full compliance with the Act to avoid any potential consequences.