Information Governance Framework

Introduction

Information Governance Framework describes the way the requirements of the following legislation and professional guidance are met within Peritus Health Management:

- Data Protection Act 2018
- Access to Medical Reports Act 1988 (AMRA)
- Access to Health Records Act 1990
- Human Rights Act 1998
- Nursing and Midwifery Council Code of Professional Standards of Practice and Behaviour (Nursing and Midwifery Council, 2015)
- General Medical Council Guidance on Confidentiality (2017)
- Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians (Faculty of Occupational Medicine, 2012)

Peritus Health Management's Information Governance Framework sets out the standards which are applied for managing information governance, including the organisational arrangements for Data Protection, Information Security and Records Management.

Particular focus is placed on the management of personal and sensitive information to ensure that it is handled legally, securely and efficiently to provide the best possible service to our customers and clients.

Information Governance Policy Statement

Peritus Health Management is committed to managing its information securely, legally, and effectively in order to provide the best possible service to its customers and clients by:

- Ensuring compliance with legal and professional duties in relation to information governance
- Protecting personal and sensitive information to ensure that the confidentiality and privacy rights of individuals are upheld and a consistently safe and ethical use of information
- Providing clear guidance on the standards and arrangements for Data Protection, Information Security, and Records Management
- Confirming the roles and responsibilities for information governance within the business
- Providing regular staff training on Information Governance and confidentiality in relation to the work undertaken and ensuring they understand the required standards for managing information as it applies to their role
- Providing suitable and sufficient resources to allow all staff to comply with the Information Governance requirements
- Implementing a robust system of audit to ensure compliance, currency, and effectiveness
- Ensuring a strong senior oversight of information governance within the business with a clear reporting structure to the Directors.

Scope

This framework applies to all Peritus Health Management staff and those who work for and behalf of Peritus Health Management.

It applies to the management and governance of all information within Peritus Health Management, and the information shared with customers as part of the service delivery, including both electronic and paper format and their associated systems.

Roles and Responsibilities

The Managing Director has overall responsibility for Information Governance and:

- ensuring compliance with legislation and professional guidance
- allocating appropriate resources to fulfil the requirements of the legislation, professional guidance and the Information Governance suite of policies
- ensuring the Information Governance suite of policies remain current
- ensuring performance of those with specific responsibilities for Information Governance and responding appropriately to concerns raised
- contracting a competent IT service provider to ensure that IT security arrangements are suitable, sufficient and consistently implemented and monitored to meet UK cyber security standards.

The Data Protection Officer (DPO) is responsible for:

- informing and advising the Directors of Peritus Health Management and its employees about their obligations to comply with the GDPR and other Information Governance legal and professional obligations and ensuring that this Policy is reviewed on a regular basis to ensure currency
- monitoring for changes in legislation and professional guidance in relation to Information Governance, undertake a gap analysis, advise the Managing Director of the changes; creating an action plan to amend business or clinical processes as appropriate in light of any changes, monitoring progress against the action plan and reporting progress to the Managing Director
- to monitor compliance with GDPR and other legal and professional obligations, including business and clinical data processing activities, advising on data protection impact assessments, managing change projects, training staff, and conducting internal audits.
- reviewing the planning for changes in services to ensure GDPR compliance is built into the process
- being the first point of contact for supervisory authorities and for individuals whose data is processed (customers, clients, employees etc)

The Operations Manager is responsible for:

- providing all new customers with information on Information Governance and ensuring the joint data sharing arrangements are clearly defined and agreed with joint controllers before the commencement of data sharing

- feeding audit data into the utilisation report in relation to the maintenance, storage and archiving of customer's client records
- auditing subcontractor's Information Governance arrangements to ensure compliance with legal and professional standards and ensuring a current data sharing agreement is in place
- ensuring all marketing activities are compliant
- ensuring data compliance of the Customer Relationship Management system

Departmental leaders are responsible for:

- ensuring all categories of personal data are identified on the Information Audit
- ensuring that the processes implemented within the department comply with the requirements of this policy and are documented in their departmental handbooks
- co-operating with the DPO and auditing processes
- reporting any concerns about the safety, security, and processing of data to the Managing Director and DPO

Employees of Peritus Health Management are responsible for:

- ensuring their compliance with the requirements of this policy and its associated procedures
- ensuring clients (patients) are provided with Privacy Notices appropriate to the services to be supplied and they understand their continued rights for confidentiality within the guiding principles of the Faculty of Occupational Medicine's Ethical Guidance (Faculty of Occupational Medicine, 2012).
- creating clinical records in accordance with the identified professional standards
- the data they process is accurate, adequate, relevant, and limited to what is necessary
- checking the accuracy of data stored and rectifying inaccurate data as appropriate
- co-operating with the DPO and auditing processes

Customers (employers) are joint controllers with Peritus Health Management as they are responsible for the referral of data subjects to Peritus Health Management and in control of information relating to:

- the data subject
- the data subject's employment status on which Peritus Health Management relies on for the retention and erasure of data
- the hazards to which the data subject is exposed, on which Peritus Health Management relies on for ensuring adequate and relevant data processing and limiting processing of irrelevant data
- the reason for the data subject's referral to or processing by Peritus Health Management

Subcontractor, such as Consultant Specialists, Occupational Physicians, Physiotherapists, Talking Therapists are also joint controllers, as they are responsible for the processing of data in relation to the referrals received from Peritus Health Management.

Peritus Health Management requires a Data Sharing Agreement to be in place to define the responsibilities for data sharing and the practical elements of compliance with all Joint Data

Controllers. This Data Sharing Agreement will be reviewed on a regular basis to ensure currency.

Monitoring compliance

Compliance with the Information Governance suite of policies will be monitored on a regular basis and feedback delivered within the Management Meeting.

Terms of Reference

Faculty of Occupational Medicine. (2012). *Ethics Guidance for Occupational Health Practice.* London: Faculty of of Occupational Medicine.

General Medical Council. (2017, January). *Confidentiality: good practice in handling patient information.* Retrieved from General Medical Council: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality#

ICO. (2011, May). *Data Sharing Code of Practice.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

ICO. (2018, March 22). *Guide to the General Data Protection Regulation (GDPR) 1.0.51.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

ICO. (Accessed 2021 , 10 21). *Report a Breach.* Retrieved from Information Commissioner's Office: https://ico.org.uk/for-organisations/report-a-breach/

ICO. (Accessed 25/10/2021). *Right to Object.* Retrieved from Information Commissioners Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

ICO. (Accessed 25/10/2021). *Right to Rectification.* Retrieved from Information Commissioners Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

Information Commissioner's Office. (2018 Version 1.0). *Data Controllers and Data Processors: what the difference is and what the governance implications are.* ICO. Retrieved from Data Controllers and Data Processors: what the difference is and what the governance implications are.

Information Governance Alliance. (2016, July). *Records Management Code of Practice for Health and Social Care 2016*. Retrieved from Digital NHS: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Nursing and Midwifery Council. (2015, January 29). *NMC Code.* Retrieved from Nursing and Midwifery Council: https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf

Revision History

Date	Revision No.	Revision description	Revised by	Authorised
25/04/2018	V1	Information Governance Policy updated following introduction of GDPR	AD	AD
18/01/2022	V2	Information Governance framework of policies created to separate different aspects making it easier to read and understand	AD / OG	AD