LATUSHEALTH

Document No:	Date Effective:	Document Title:
HR.03.001	29 Apr 20	Confidentiality

Approvals

The electronic signatures below certify that this policy has been reviewed and accepted and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

	Signature	Position	Date
Prepared by:	 Victoria Tait	Quality Specialist	15 Apr 20
Reviewed by:	 Will Latus	Director	29 Apr 20
Approved by:	 Will Latus	Director	29 Apr 20

Amendment Record

This policy has been reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

Page No.	Context	Revision	Date

Document No:	Date Effective:	Document Title:
HR.03.001	29 Apr 20	Confidentiality

1. SCOPE

This policy applies to all (both clinical and non-clinical) Latus Health Ltd. (the "Company") employees. This includes anyone who has agreed that they have a duty of confidence, and has access to clinical systems, and patients', staff and/or organization confidential or business sensitive information. This will include but not be limited to all employees of the Company, partner organisations who access record systems and contractors.

2. PURPOSE

This policy is designed to provide realistic guidelines concerning confidentiality of information received by the Occupational Health Team, whether it is information from the employees or about the organisation and its' processes. This policy applies no matter how the data is processed or stored; electronically, documents, images, paper records.

3. BACKGROUND

This policy sets out the Company's commitment to ensuring any personal data it processes as part of its operations is conducted under a strict code of confidentiality, in accordance with 'Data Protection Law'; this includes the General Data Protection Regulation; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation. The Company ensures that good data protection practice in line with applicable GMC guidance on confidentiality is imbedded in the culture of our staff and our organisation.

Under the terms of these legislations, the Company will hold various types of data including we process personal and special category data relating to our staff and those we treat internally and with other organisations external to the practice. We also hold data on employees, customers, suppliers, business contacts and other people we have relationships with or may need to contact. The Company acts as the 'data controller' under the Act and fully endorses the need for and agrees to process this data solely according to the Act. These processing activities, and others, are described in detail in our company **Privacy Statement_BM.01**.

The Nursing Midwifery Council, Code of Professional Standards states that as a nurse, midwife or nursing associate, has a duty of confidentiality to all those who are receiving care. This includes making sure that they are informed about their care and share necessary information with other health and care professionals and agencies only when the interests of patient safety and public protection override the need for confidentiality.

However, all of the professions we regulate exercise professional judgement and are accountable for their work. Nurses, midwives and nursing associates uphold the Code within the limits of their competence. This means, for example, that while a nurse and nursing associate will play different roles in an aspect of care, they will both uphold the standards in the Code within the contribution they make to overall care. The professional

commitment to work within one's competence is a key underpinning principle of the Code which, given the significance of its impact on public protection, should be upheld at all times. In addition, nurses, midwives and nursing associates are expected to work within the limits of their competence, which may extend beyond the standards they demonstrated in order to join the register.

Preservation of confidential relates to information about employees of clinical, social or personal nature obtained verbally or recorded in written or computerised form. An important distinction used to be made between this kind of information, which is confidential and information representing opinion, advice or interpretation of facts, which is not. Under GMC requirements, clinicians should not disclose any sensitive information, which includes medical or professional opinions to anyone without the express consent of the individual, except with the above provisos above in quotes.

4. RELEVANT LEGISLATION, STATUTORY BEST PRACTICE AND DATA PROTECTION PRINCIPLES

The Common Law Duty of Confidentiality is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent unless there is an over-riding public interest (e.g. public health) or legal duty to do so (e.g. detection or prevention of serious crime). The UK Data Protection Act – DPA (1998) controls how an individual's personal information is used by organisations, businesses or the government. The Company will register with the Information Commissioner's Office on an annual basis. In May 2018, the DPA was repealed by the European Union General Data Protection Regulation (GDPR). The overall principles of the GDPR are for organisations to be fair and transparent about how they use individuals' personal information, and for individuals, where possible, to have more choice and control over how their personal information is used. GDPR builds on current law and best practice. GDPR requires that the company identifies the legal basis for processing, managing and sharing patient information. Data protection legislation applies only to living individuals, who have a right to access information that an organisation holds about them. The Company complies with the data protection principles set out detail in our company **Privacy Statement_BM.01**.

5. RESPONSIBILITIES

Everyone who works for the Company or with us has shared responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data in this organisation must ensure that it is handled and processed in line with this policy and data protection principles.

The following specific duties and responsibilities apply within the Company:

- The Directors have overall responsibility for the Confidentiality Policy.
- The Directors are responsible for ensuring all staff are aware and comply with this policy.

- The Data Protection Officer will be responsible for providing advice, liaising with other organisations to process subject access requests, coordinating the release of the data and investigating complaints.
- The Directors are responsible for ensuring systems, services and equipment used for storing data meet the company confidentiality and security standards. Regular checks and reviews are performed to ensure security hardware and software is functioning properly. The Company ensures that cyber security recommendations are implemented and deployed, and continual staff awareness is raised regarding cyber security.

All Company staff are responsible for ensuring that:

- Their own personal data provided in relation to their employment is accurate and up to date
- Person identifiable data that they handle lawfully as part of their role is as accurate and up to date as possible, kept securely with restricted access, and not kept for longer than necessary.
- All staff, including contractors and agency staff are responsible for person identifiable data that they record or process and are obliged to adhere to this policy.
- All staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised. Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of the Company's data protection policies may also be a criminal offence.
- All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to. All requests will be considered without undue delay and within one month of receipt as far as possible.
- All staff are responsible for ensuring that personal or sensitive data is held securely and that it is not disclosed to any unauthorised third party. Data that is disclosed inappropriately or accidentally must be reported to the Data Processing Lead. Any reportable breaches will be reported to the ICO within 72 hours where possible. All data breaches will be examined, whether reportable or not, to ensure measures are put in place to prevent recurrence, to reduce risk, and to ensure lessons are learned.

6. PROCEDURE

6.1 Access to health records. The records should be kept in a locked system, paper or electronic and the responsibility for which should be with the Occupational Health Nurse/authorised Administration Personnel. Original paper health records will not normally be allowed to leave the department. Exceptions to this are during an Occupational Health Nurse visit to departments for a client conference or copies of records to be given to the Company Clinical Staff working at the client premises.
Records should:

* Not be left unattended on desks when not in room
* Not be duplicated and/ or transported unless necessary
* Not be left overnight in unlocked cabinets

Access to personal records should be confined to staff within the Occupational Health department. No employee or executive of an organisation external to the Occupational Health Team should be given access to the health records unless it is with the written consent of the employee to whom the contents refer. The employee should be aware of the reason for agreeing to the release of his/her occupational health records and provide written consent.

7. PROCEDURE FOR DISCLOSURE TO THIRD PARTY

7.1 Copies of entries and reports from the medical file requested by an individual, or their authorised representative, must be released if requested under the Data Protection Act or the GDPR. Previous disclosures requested under old legislation like Access to Medical Records Act have largely been superseded and would not normally be expected now. These placed limits on access to those records written after 1991 whereas now all historical records can be requested.

7.2 Health records can be withheld where the information is likely to cause serious harm to the physical or mental health of the subject or any other person e.g. where a confirmed or suspected medical diagnosis is recorded but currently unknown to the client.

7.3 If the information relates to or has been provided by a third party other than the health professional, and this could identify the person concerned, consent must be obtained prior to the release of any documents. Alternatively, references to the third party can be blocked out before sending.

7.4 In some cases, the file copies are requested by and sent to an agent or adviser, not the client. Without consent, or a court order, no information, written or verbal can be disclosed.

7.5 Any confidential information concerning clients obtained and recorded in the course of professional practice can only be disclosed to a third party e.g. manager, solicitor.

7.6 Where the disclosure of some confidential information to a third party is required in order to fulfil the service provided by the Company, this will be made clear to the individual concerned and consent for this will be attained.

* With the consent of the client

(This must be done in writing and the client must understand precisely what information will be disclosed)

Or if consent is not given

* If it is required by law

There are a number of statutory provisions that require disclosure of information to a public body e.g. The Prevention of Terrorism Act, The Health and Safety at Work etc. Act 1974, The Road Traffic Act or a formal court order

* If it is unequivocally in the public interest
* *If it is necessary to safeguard national security or to prevent a serious crime*
* *If it will prevent a serious risk of public health*
* *If certain circumstances for the purpose of medical research (Faculty of Occupational Medicine 1993).*

Should a member of the Occupational Health department become involved in a case of litigation between a client company and their employer, this should be discussed with the Occupational Health Physician and Occupational Health Nurse Manager, who may seek legal advice before following a course of action.

8. ACCESS TO MEDICAL REPORTS ACT 1988

8.1 Under the Access to Medical Reports Act, it shall be the right of an individual to have access, in accordance with the provisions of this Act, to any medical report relating to the individual which is to be, or has been, supplied by a medical practitioner for employment purposes or insurance purposes. Anyone commissioning a report for such purposes must obtain the consent of the client who is the subject of the report. The client then has the right to see the report before it is sent. This right remains for six months. The Act only applies to reports written after 1 January 1989.

8.2 The employee has the right:

- To withhold consent to the application being made
- To state that he/she wishes to have access to the report before or after it is supplied to the employer
- To be informed in writing when the report has been requested
- A request to see the report, before being supplied to the employer, should
- be made within 21 days of being notified that the request has been made
- To withhold consent to the report being supplied to the employer
- To request amendments or attach a statement to the report if he/she feels it is incorrect or misleading.

8.3. This Act is still sometimes referred to especially if the organisation has old consent forms. Technically it makes little difference to the Company when we are requesting reports from GPs or consultants. It should never now be used when companies are recurring reports from the Company as this has been superseded by GMC guidance on confidentiality which does not specify a period of 21 days but insisted everyone should be offered

a copy of their report and there should be no surprises when they receive it. The Company doctors are encouraged to dictate reports in front of the client so they can hear what advice is being given.

9. CHANGES TO SYSTEMS AND PROCESSES – DATA PROTECTION IMPACT ASSESSMENTS

It is important that changes to services and systems and processing of person identifiable data are assessed to ensure that confidentiality, accessibility and integrity of data are maintained.

10. RECORD KEEPING

10.1 Access to Company Policies and Procedures will be given at Induction. This policy will be monitored biennially by the Company to review its effectiveness and will be updated, and employees notified in accordance with any necessary changes.

10.2 Data is stored securely on 'Cohort' software system provided by Medgate UK. A copy of their data protection policy and storage parameters can be accessed: http://cohort.medgatesoftware.co.uk/privacy-policy/

11. DOCUMENTATION

https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf
http://www.legislation.gov.uk/ukpga/1988/28/contents