Management of Confidential Information and Sensitive Data

May 2018

Procedure and Instruction Details

Author/Job title	Amanda Batey, Director A.B. Health Ltd		
Responsible Officer			
Reviewed by			
Approved by	Dr Michael Coolican, Director Company Medical Ltd		
Frequency of review	3 Yearly or after changes to legislation		
ID Number		**For Use**	Internally
Location			

Version history

Version number	Summary of change	Author	Date
0.1	Drafted for Approval	Amanda Batey	01-05-18
0.2	Approved Document	Dr Mike Coolican Amanda Batey	30-11-18

Definitions and Abbreviations

Breach of Confidentiality	In relation to this policy and procedure, a breach of confidentiality is a disclosure of confidential information / sensitive data, outside OH, without employee/client consent, court order or legal justification. Disclosure can be oral or written, by telephone or fax, or electronically, e.g. via e-mail. Any breaches of confidentiality may be considered as gross misconduct and therefore likely to result in disciplinary action.
OH / OHS	Occupational Health / Occupational Health Service
Clinical Audit	Evaluation of clinical performance against standards or through comparative analysis, to inform the management of services. Studies that aim to derive, scientifically confirm and publish generalisable knowledge constitute research and are not encompassed within the definition of clinical audit in this document.
Consent	Agreement to an action based on knowledge of what the action involves and its likely consequences.
Express consent	Consent which is expressed verbally or in writing
Implied consent	The assumption a person has consented to something by his/her actions. This means that, although the person has not given verbal or written consent, circumstances exist that would cause a reasonable person to believe the other had consented.
Health care team	The health care team comprises the people providing clinical services for each patient and any administrative staff who directly support those services.
Public interest:	The interests of the community as a whole, or a group within the community or individuals.
OH file / record	Occupational Health record is anything that contains information (in any media) which has been created or gathered as a result of any aspect of the OH Medical Practitioner's work relating to clients. The record may contain information about the current episode only or may be a compilation of every episode for that individual. A record must be kept of every visit/contact. Any part of a record held must comply with the Data Protection Act 2018.

Contents

1. Introduction

The provision of a confidential, informed and impartial service to external client's and the organisations who use the Occupational Health Service is essential to maintain a professional relationship of trust and also compliance with legislative requirements namely the Data Protection Act 2018 and professional codes of practices and ethics.

A.B. Health Ltd holds information about employees/clients which is private and sensitive. Some of this information is classified as medical information or special categories of personal data, under relevant legislation. This information / data must not be given to others unless the employee/client consents to do so, or the disclosure can be justified.

Particular regard shall be given by all A.B. Health Ltd staff to 'confidentiality', 'consent' and 'disclosure' in the course of their work and they are required to comply with this policy and their own professional codes of practice / conduct, as applicable.

2. Scope

The law applies to the processing of personal data by electronic means and of manual data which forms part of a filing system. This policy and procedure is applicable to all A.B. Health Ltd staff and it is a mandatory requirement that staff comply with its requirements. Breaches of confidentiality or disclosure of confidential information / special categories of data, both intentionally or unintentionally, may be considered as gross misconduct and likely to result in disciplinary action.

The Company could be subject of fines for breach of the law up to 4% of annual turnover.

This policy and procedure affects all employees and clients who use A.B. Health Ltd.'s services, who have a right to expect that personal data / information about them will be held in confidence, unless they consent to release it.

This policy and procedure also affects others who information is provided to, due to the nature of their work or involvement with A.B. Health Ltd, e.g. Human Resources (HR) staff. This information will be private and confidential management information only when consent is provided by the individual. People who obtain any information from A.B. Health Ltd must consider and use this information sensitively in accordance with relevant legislation and in order to respect the rights of the individual employee / client.

3. Responsibilities

The Directors of A.B. Health Ltd are responsible for maintaining this policy and overseeing its acceptance and compliance, including the security of the information contained in Occupational Health (OH) records and for making sure that access to the information held is appropriate and is closely supervised. For the purpose of the Data Protection Act 2018, the Directors are deemed data controllers i.e. the person who determines the purpose and means of the processing of personal data, in addition to data processors.

All other staff of A.B. Health Ltd are deemed to be data processors as they process data on behalf of the Directors of A.B. Health Ltd. They are responsible for complying with this policy and their own professional codes of practice / conduct, as applicable. All staff will be required to sign a confidentiality agreement to this effect. Additionally, after employment with A.B. Health Ltd no information or sensitive data obtained during the course of employment with A.B. Health Ltd can be disclosed to any person or taken from A.B. Health Ltd and thereafter made use of.

4. Lawful Basis for Processing

4.1 The processing of data within A.B. Health Ltd is in relation to data pertaining to health which is deemed special category data. All data will be processed in conjunction with Article 6 and Article 9 of the Data Protection Act 2018. The employer for which A.B. Health Ltd is contracted will also need to process health data i.e. obligations to pay sick pay and they need to monitor sickness absence. The employer also has a duty under Health and Safety Law and may have to institute and keep records of statuary health surveillance. In performance of these duties the employer may refer workers to A.B. Health Ltd and act upon information documented in the reports; they will therefore be required to demonstrate their own lawful basis for processing.

4.2 Article 6 states that processing is only lawful if one of the conditions in Article 6(1) is met**.** As an independent, OH provider A.B. Health Ltd will deem paragraph (f) as the lawful basis for processing; “Processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interest of fundamental rights and freedoms of the data subject which require protection of personal data.”

4.3 As A.B. Health Ltd deals with health data it requires a lawful basis for processing under Article 9 in order to justify processing special category data. A.B. Health Ltd lawful basis of processing under this article is deemed to be Paragraph (h) “Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, and the provision of heath care”

4.4 The data controller must inform the data subject of the lawful basis for processing personal data.

5. Policy Statement

5.1 A.B. Health Ltd will respect the confidentiality of employees and clients (including deceased employees and clients) and will maintain and protect the special categories of data / information it obtains about employees and clients, as part of its undertaking, in accordance with relevant legislation and best practice.

5.2 Certain information obtained concerning an employee’s / client’s general health and the resulting impact on work abilities, including any individual based risk assessments, may be shared with management, Human Resources and other members of the health care team, as applicable, taking into account the amount of information permitted by the express consent of the individual involved.

6. Recording and Storing of Sensitive Information and Data

6.1 A.B. Health Ltd has been registered with the Information Commissioners Office (ICO) as a Data controller since 13th May 2011. Registration number Z2671608

6.2 OH records can be the property of the company or organisation. However, there is a clear distinction of ownership of the records and the right of control over their information content. The information contained within the OH records at A.B. Health Ltd belongs to the Occupational health professionals. Employees of A.B. Health Ltd have the duty to protect the confidentiality of the data subject and ensure OH records and any information held are only accessed with the express consent of the data subject involved or via a legal or appropriate public interest obligation.

6.3 Information and data regarding an individual can be obtained via email, land mail or telephone from a referring organisation or entity and during a clinical assessment of the individual which can either take place over the telephone or in a face to face appointment.

6.4 Information held by A.B. Health Ltd consists of management communications and referrals as well as clinical information gained through a direct clinical assessment along with the resulting Occupational Health reports generated on the basis of this process. In addition to this Specialist or General Practitioner medical reports can be obtained with the written consent of the individual involved. Such documentation can include sickness absence history, and a record of medical and health issues and highly sensitive personal data. A.B. Health Ltd takes its professional, ethical and legal obligations in relation to data protection and security with the utmost seriousness and will process and protect all personal data lawfully, fairly and in a transparent manner.

6.5 Paper-based and electronic information will be held securely at A.B. Health Ltd registered office

6.6 During assessments carried at some client's sites, files may have to be removed from A.B. Health Ltd on the day and then returned in the evening. In these circumstances files and records will be held in a locked case to prevent unauthorised access to them and will not be left unattended.

6.7 All paper-based and confidential records are to be kept in lockable secure cabinets whilst at A.B. Health Ltd Registered Office. Paper-based records are kept in accordance with the 8 principles set out in the Data Protection Act 2018, and will be destroyed when no longer required or at the end of the retention period as appropriate.

6.8 Electronic Records**.** A.B. Health Ltd stores data on a dedicated Computer which is protected from unauthorized access and is password protected. Up to date anti-virus software is installed along with the scope for VPN connection. Paper records are now scanned into a secure area of the computer and encrypted using bit locker drive encryption methods. OH reports are password protected when sent by e-mail

7. Information and Record Retention Policy

7.1 Paper based records of confidential information will be maintained in accordance with A.B. Health Ltd records register and retention schedule. This schedule is that such information will only be kept as long as there is a justifiable purpose for doing so. The current recommendations and guidance are they will be kept for as long as the employee is employed by the referring organisation and then for a further 6 years up to their 75th birthday, whichever is sooner. For contracts that have been terminated and notes not transferred to another provider, records will be stored securely for 6 years after the last entry and then destroyed, unless they are pertaining to health surveillance when the guidance from the Health and Safety executive is that they be kept for 40 years.

7.2 Paper records will be destroyed by the use of cross cut shredder in a secure manner as confidential waste

7.3 Electronic records will be permanently deleted in a secure manner from the A.B. Health Ltd computer system in accordance with the A.B. Health Ltd retention schedule.

7.4 Pre-Employment forms where the individual did not take up the post will be kept for 1 year and then securely destroyed.

7.5 Records of deceased employees/clients will be retained for 10 years in accordance with pension requirements, Department of Health recommendations and the Access to Health Records Act.

8. Data Subject Access Request

8.1 Individuals have a right to view or have copies of any information held in their OH record under the Data Protection Act 2018 (DPA), providing the information does not disclose information about a third party other than a professional involved in the case. If a third party is identified then that person's permission should be sought or the notes redacted to remove the third-party information.

8.2 With any subject access request the Director of A.B. Health Ltd will need to be immediately informed

8.3 Before allowing access, explicit written consent must be received from the employee/client who should then arrange a suitable time to view the file/record or if requested a copy of the information should be sent by recorded secure delivery. This process must be completed within a maximum of 28 days of the signed request and consent being received.

8.4 Before the viewing or the sending a copy of the information, the file should be checked by the Medical Director of A.B. Health Ltd and any irrelevant information, information that identifies another individual (that would breach his/her confidentiality) or information that could cause serious harm to the physical or mental health of the employee/client or someone else, should be withheld, in accordance with the provisions of appropriate legislation.

8.5 If viewing the data, the employee/client's identity should be checked/verified before handing over the file. The employee / client should be offered a quiet area in which to view the file/record and they should be supervised during this time.

8.6 On either viewing or receiving a copy of their data and information If the employee/client believes any information in the file is inaccurate, they can add a statement to the file to this effect and offer any information which they believe to be correct.

Note: Where an access request has previously been complied with, the DPA permits record holders not to respond to a subsequent identical or similar request unless a reasonable interval has elapsed since the previous compliance.

9. The Occupational Health Consultation and Consent

9.1 Types of consent

Informed consent - This is ensuring that the individual is provided with sufficient information regarding the nature and purpose of the OH process and consultation and the potential consequences of it. As part of achieving informed consent, the employee must be advised with whom their personal information is being shared and the purpose for which it is being shared. The employee should also be informed if any referral for intervention e.g. counselling / physiotherapy is being recommended or is made and what information is intended to be shared for this.

Implied consent – The inference that the individual is consenting to proceed with the consultation without any formal documentation. Verbal consent from the employee / client will be enough in most cases for care and support to continue or be withdrawn. At any stage during the OH process an individual may refuse or withdraw their consent either verbally or in writing.

9.2 Written **informed** consent must be obtained prior to the Occupational Health consultation commencing. All clients attending for occupational health consultation should be issued with a A.B. Health written consent to proceed form. This consent form contains the A.B. Health Ltd Privacy Notice and informs the individual on how the information they provide to A.B. Health Ltd will be used

When obtaining consent, the following must be provided:

- An explanation of what information is needed or recorded and why, and what uses may be made of it;
- a description of the benefits that may result to the individual from the proposed use or disclosure of the information;
- how the information obtained and how its uses will be protected and assured;
- any outcomes, implications, or risks, if consent is subsequently withheld.
- An explanation that any consent can be withdrawn in the future (including any difficulties in withdrawing information that has already been shared).
- an indication of the patient's right to see a copy of the OH report prior to it being sent to the referring organization or entity and that the employee has a right of access to all information held on them by A.B. Health Ltd

9.3 During contact / consultation with clients, Medical Practitioners should ensure employees / clients are aware of requirements surrounding medical confidentiality and consent, and that a confidential management report will be produced for HR and/or Manager. It may be necessary on occasions to disclose some part of an individual's medical history for example when a manager has requested information regarding fitness for work and implementation of the Disability Provision of the Equality Act. In such circumstances the practitioner must always discuss the disclosure and obtain their informed consent prior to sending the report.

9.4 Only required information will be collected and will only be used for the purpose it is obtained.

9.5 The Medical Practitioner should inform the employee / client of the content of the OH report and offer a copy of the report for viewing before it is sent to the employer and if the employee / client disagrees with the Occupational Physicians opinion, inform them that they can add an addendum to the report highlighting this issue and the reasons for the disagreement. OH reports will provide impartial opinions and advice only. It is important to advise the individual that consent for release of the report and information can be withdrawn at any time.

9.6 Following or during any contact / consultation / appointment with the client, the Medical Practitioner will record appropriate file notes for medico legal purposes

9.7 A report will be completed following the consultation and sent to the referring party, this will be sent via an encrypted system or via a password protected document. If on client sites the report will be stored on a shared I.T. drive with Human Resources (HR), where only the relevant HR personnel will have authorised access. A printed copy of the report will always be placed in the employee's OH file

9.8 Employees of the organisations will be sent a copy of any management report provided by OH directly or via their Departmental HR Officer at their request or will be provided with a copy by A.B. Health Ltd

9.9 If a GP / Specialist report is required, the Medical Practitioner will obtain expressed written consent, in keeping with the provisions of the Access to Medical Reports Act 1988, during the consultation, on the relevant form. This gives extra rights to the individual in that they can document if they wish to review the report before its released by the GP / Specialist.

9.10 Sharing information in the health care team. Clients should be informed that medical information provided in confidence to an OH Practitioner may need to be shared within the occupational health care team in order to provide on-going employee/client support, assessment or case management progression. The member of clinical staff should make sure the individual understands how and what level of information will be shared. Consent should be obtained to share this information and documented on the relevant form.

9.11 Employees / clients occasionally feel the need to be accompanied during OH consultations, by a trade union representative or a work colleague or family member / friend. A.B. Health Ltd will require employees/clients to provide explicit oral or written consent to do so. The practitioner should inform the parties that sensitive personal information will be sought and discussed during the consultation, thus ensuring the employee / client is happy

to discuss this in the presence of the person they have brought. Once consent is provided the OH Practitioner will consider whether to see the employee/client with the companion. In exceptional circumstances the OH Practitioner may not agree to see the employee/client with the companion, in which case he/she will inform of the reasons for his/her decision.

10. Procedures for maintaining confidentiality and data protection

10.1 During the course of employment with A.B. Health staff members will have access to, gain knowledge of, or be entrusted with medical or personnel information concerning individual clients. The information will include matters of a highly sensitive and personal nature.

10.2 It is required that A.B. Health staff respect the rights of confidentiality and data protection for all its clients.

10.3 All Medical and nursing staff work within a strict code of ethics concerning the confidentiality of consultations and medical records.

10.4 All staff of A.B. Health Ltd will be requested to sign a confidentiality agreement in relation to accessing and processing occupational health notes/records /reports. By signing the agreement, the employee acknowledges that they will not at any time, whether during or after employment with A.B. Health Ltd, divulge or disclose to any person or otherwise make use of such confidential information.

10.5 All staff should be careful not to unintentionally disclose confidential information whilst in employment with A.B. Health Ltd. Computers should not be left switched on and unattended without being password protected. Occupational health files, records or data should never be left unattended or used in areas where they can be easily viewed by others who are not authorised to view the data / information (e.g. public transport or café's etc).

10.6 Extra care should always be taken when seeing clients in areas where confidential information is being used or viewed.

10.7 Staff should not discuss identifiable employees or clients where they can be overheard or leave any OH records or confidential information, either on paper or on screen, where they can be seen by other individuals or the public.

10.8 When using computers A.B. Health staff shall

- Always log-out of the system/application when work on it is finished
- Not leave a PC/laptop unattended and logged-in / unlocked.
- Not share logins with other people. Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Always clear the screen of a previous patient's information before seeing another.

10.9 When using mobile phones or tablets for Company business ie for dealing with e-mails, particular care needs to be given to;

- Appropriate security password protection for the device
- Use of up to date anti-virus software installed on the device

- VPN encryption when connecting to a public Wi-Fi network
- After reading e-mail correspondence containing sensitive information consider deleting the e mail and information from the device after use, as the e-mail will also be on the main A.B. Health Ltd computer account where it can be more securely stored
- If any sensitive documents or information are stored on the device, store in a secure password protected folder and then delete from device when not needed
- Be aware of phishing e-mail scams
- Take care with opening attachments from unknown e-mails as these may contain viruses or malware

10.10 When appropriately disclosing any information, care must be exercised to ensure this can be done safely and securely:

- Information must only be disclosed to the right person with appropriate consent having being given. Staff should check that any callers, by telephone or in person, are who they say they are. If unsure, seek official identification or check identity by calling them back on an official number. Always check that they have a legitimate right to access the information requested.
- Ensure that appropriate standards are applied in respect of e-mails i.e. password protected documents, and also that this is the correct media for sending the information. Double check e-mail address before sending to ensure it is the right recipient and no inappropriate copies have been sent
- Ensure that appropriate standards are applied in respect of faxes and that the authorised receiver has confirmed that are waiting at the other end to receive the information on transmission of the fax.
- Ensure that appropriate standards are applied in respect of mail/post and also that mail is appropriately sealed/secured and correctly named and addressed. A confidential stamp should be used on the envelope as appropriate. Reusable envelopes must not be used. Any manual/paper based medical information / sensitive data should be sent secure means which is tracked through the mail or courier system and signed for on receipt. Examples include Special Delivery or Recorded Delivery
- The minimum amount of information should be disclosed to satisfy the purpose. It is important to consider how much information is needed before disclosing it. This must clearly be balanced against the need to maintain the health or safety of an individual(s), where missing information could be dangerous.

10.11 Disclosing information with informed consent to a Third Party

An employee may request that A.B. Health Ltd sends information from their OH file to a third party, e.g. a solicitor or another OH provider. Information should only be sent with written consent, stating what information is to be sent and to whom. All requests for disclosure should be dealt with by a Director of A.B. Health Ltd. The consent for release should include the following:

- Name (printed)
- Date of Birth
- Signature
- Name and address of person the information is to be sent to

Information should only be disclosed when the practitioner is satisfied that the consent is indeed that of the individual concerned. Information will not be released if authorisation is in the form of a photocopy or faxed authorisation, an original signature is required.

On occasions Human Resources or line managers may try to request access to an individual's OH record, possibly as part of an investigative hearing. The person requesting the information must obtain and then supply the individual's fully written and informed consent before any information can be disclosed.

Disclosure to Solicitors

Most contacts from solicitors are for subject access requests for copies of occupational health records for compensation claims. Explicit written consent should be obtained before disclosure unless a court order is received. Often a solicitor provides consent via their own form and this should be checked carefully to ensure it is appropriate. Ideally disclosure should be limited to the incident concerned; however, if disclosure of the full record is required this should be complied with. Before copying the file, this should be checked by the Director of A.B. Health Ltd beforehand and any information, information that identifies another individual (that would breach his/her confidentiality) or information that could cause serious harm to the physical or mental health of the employee/client, should be withheld, in accordance with legislation. Original documentation must not be sent only appropriate photocopies.

Disclosure to the Courts, including Coroner's Court and Tribunals

The courts, some tribunals and persons appointed to hold enquiries have legal powers to require disclosure of confidential information. If an OH professional is required to give evidence in any court proceedings, then they cannot withhold confidential information. If information is withheld it is contempt of court and punishable as a criminal offence. Care however needs to be taken to limit disclosure strictly in terms of the relevant order, the precise information requested to the specified bodies and no others. It is permitted to make ethical objections known to a judge or presiding officer, but unless the order is changed compliance is necessary. Before any such disclosure the Director of A.B. Health Ltd must be informed.

Disclosure to the Police

Whilst the police have no general right of access to health records there are a number of statutes which require disclosure to them and some that permit disclosure. These have the effect of making disclosure a legitimate function in the circumstances they cover. In the absence of a requirement to disclose there must be either explicit consent or a robust public interest justification. What is or isn't in the public interest is ultimately decided by the courts; however A.B. Health Ltd will consult with their Medical Indemnity Defense Organisation (MDDUS) and follow the advice of their legal services in such instances. Where disclosure is justified it should be limited to the minimum necessary to meet the need and the employee/client should be informed of the disclosure unless it would defeat the purpose of the investigation, or allow a potential criminal to escape or put staff or others at risk. Before disclosure a Director of A.B. Health Ltd must be informed.

Disclosure to Members of the Public or the Media

Under normal circumstances there is absolutely no basis for any disclosure of confidential information to members of the public or the media. There may be rare occasions however when A.B. Health staff may be asked for information in general terms or about employees / clients, e.g. in distressing circumstances. Care must be taken to avoid breaching any confidentiality whilst dealing sympathetically with requests for information. Where practicable, the explicit written consent of the individual concerned should be sought prior to disclosing any information. A.B. Health will access legal advice and advice will be taken from the Medical Indemnity Defense Organisation (MDDUS), where information is already in the public domain, placed there by individuals or by other agencies such as the police. These requests and circumstances must be managed by the Director of A.B. Health Ltd.

10.12 Disclosing information to a third party without any Consent

In exceptional circumstances, OH records can be released to third parties without consent. These circumstances are:

- It is required by law
- If disclosure is clearly in the patient's interest but it is not possible or is undesirable to seek consent.
- It is in the public interest.
- It is necessary to safeguard national security or to prevent a serious crime.
- It will prevent a serious risk to public health
- In certain circumstances for the purposes of medical research.

In all instances these cases will be managed by the Director of A.B. Health Ltd and advice sought from the Medical Indemnity Defense Organisation (MDDUS)

10.13 Access to a deceased employee/client's record

When an employee/client has died, their personal representative, executor, administrator or anyone having a claim resulting from the death has the right to apply for access to the deceased's OH record under the Access to Medical Records Act 1990. On checking the file, if the OH Practitioner identifies that the deceased person had indicated that they did not wish information to be disclosed, or the record contains information that the deceased person expected to remain confidential then it must remain so. In addition, the record holder has the right to deny or restrict access if it is felt that disclosure would cause serious harm to the physical or mental health of any other person, or would identify a third person.

11. Implementation and Operation

11.1 This policy will come into immediate effect as official A.B. Health Ltd policy and will be formally reviewed in 3 years or sooner if relevant legislation changes require

11.2 Failure to comply with this policy and procedure will result in a breach of confidentiality and data protection, which will be considered a gross misconduct and liable to disciplinary action.

11.3 If any member of OH staff identifies a data, information or confidentiality breach, possible breach or risk of breaches then he/she must raise these concerns immediately and without delay with the Director of A.B. Health Ltd who will then undertake a full investigation and take any necessary remedial action identified as necessary.

References

References

- Common Law Duty of Confidence
- General Data Protection Regulations (2018)
- Access to Medical Reports Act 1988
- Access to Health Records Act 1990
- Human Rights Act
- Freedom of Information Act
- Department of Health (1998) *Guidance for Access to Health Records Requests under the Data Protection Act 1998* DoH
- Department of Health (2004) *Confidentiality NHS Code of Practice* DoH
- RCN (2005) *Confidentiality (Guidance for Occupational Health Nurses)* London RCN
- Green, S. J (2005) *The Essential Medical Secretary – Foundations for Good Practice*, *2nd Edition,* AMSPAR, Bailliere Tindall
- Faculty of Occupational Medicine (2012) *Ethics Guidance for Occupational Health Practice,* Faculty of Occupational Medicine, London
- British Medical Association (2007) *Guidelines on Access to Medical Reports* BMA
- Lewis, J and Thornbory, G (2006) *Employment Law and Occupational Health, A Practical Handbook* Blackwell Publishing
- Faculty of Occupational Medicine (2007) *Fitness for Work – The Medical Aspects, 4th Edition* Oxford University Press
- NMC (2015) *The Code – Professional Standards of practice and behaviour for Nurses and Midwives (Advice for Nurses and Midwives)* NMC

Appendix
Legal Framework - Summary of the Law

There are several key pieces of legislation that address confidentiality and disclosure which A.B. Health staff must familiarise themselves with. A brief outline of the legislation is given below. Detailed guidance on the interpretation of the legislation can be found in the documents listed in the reference list.

Common Law Duty of Confidence

The common law duty of confidence is summarised in the case *Attorney General v Guardian Newspapers Ltd No 2 [1990] 1 AC 109*. It arises when confidential information comes to the knowledge of a person or organisation in circumstances where it would be unfair for the information to be disclosed. The courts have held that the duty of confidence only applies to information not already in the public domain and it does not apply to information which is trivial. The duty that confidence should be preserved may be outweighed by some other public interest factor which favours use or disclosure, either to the world at large or to the appropriate authorities.

Data Protection Act (2018)

The Regulations places responsibilities on employers to process the information they hold in a fair and proper way. It covers all computerised and paper records and personal data.
Data that is obtained and held is required to be accurate and where necessary kept up to date. It should be kept secure and handled in accordance with the Regulations. It should also not be held for longer than is necessary. Individuals have a right to access any personal data held.

Access to Medical Reports Act

The Act establishes a right of access by individuals to reports relating to themselves provided by medical practitioners for employment or insurance purposes. The Act outlines the consent process for supplying a report and any correction of errors.

Access to Health Records Act

This Act, which gave access to manually held medical records, has now been repealed save for the access to health records of the deceased. This right of access is negated however if the individual concerned requested that a note denying access be included within the record prior to death. Records of living persons now fall in the protection of the Data Protection Act.

Human Rights Act

This Act aims to ensure everyone's rights are properly respected, taking into account relevant laws. Article 8 of the European Convention on Human Rights (from which the Human Rights Act was derived) defines the right to respect ones private and family life, home and correspondence. This includes the right to have medical information, kept private and confidential, unless there is a very good reason not to.

Freedom of Information Act

This Act allows the majority of recorded information held by public authorities to be accessible to everyone (who requests it). If the information requested relates to an individual, this will be handled under the Data Protection Act instead of the Freedom of Information Act.