Control Manual

For

Management of Medical Records

Issue No	Issue Date	Author	Reviewed By	Approved By
16	26.03.18	Margaret Laurie	Margaret Laurie	Margaret Laurie

0: Contents

1: Purpose 3

2: Scope 3

3: Responsibility 3

4: Procedure 3

5: Related Documants 7

1: Purpose

Return to contents page

1.1: To ensure all personnel responsible for medical records and information contained therein, abide by the Nursing & Medical Professional Code of Conduct, Access to Health Records Act 1990, General Data Protection Regulation (GDPR), Access to Medical Reports Act 1988 and Fusion OH procedures.

1.2 GDPR Article 6.1 Lawful Processing
(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

1.3 GDPR Article 9.2 Processing of special categories of personal data
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

2: Scope

Return to contents page

2.1: Applies to all Fusion Occupational Health Clinicians /Technicians/Administration assistants.

3: Responsibility

Return to contents page

3.1: The Clinical Director (Data Protection Officer) has overall responsibility for data and quality control. For contracts, the relevant Director or Manager has overall responsibility of documentation and the Director of Services is responsible for staff being fully conversant with the equipment, software, operational, service and calibration requirements specified by the organisation.

3.2: Each individual is responsible for his or her own professional practice and has responsibility to ensure that legislative standards relating to control of medical records/sensitive personal data and Fusion processes are met, failure to do so may result in internal disciplinary measures been taken against the individual and/or involvement of the respective professional bodies. This policy and procedure exists to supplement this requirement

3.3: Electronic data back-ups, electronic mail and virus controls are the responsibility of the Director of Services.

4: Procedure

Return to contents page

4.1: Confidentiality

4.1.1 Confidentiality arises in a professional relationship where one person makes a disclosure of information to a professional in the expectation that the information is essential to the relationship and will remain confidential. This means that the information will not be passed to another person without the permission / consent of the individual concerned.

4.2: Medical Records

4.2.1: A file containing all medical information received regarding Fusion employees and employees of Client Companies must be kept in a locked environment, with the keys held by an Occupational Health professional or if stored in an electronic version in a secure, limited access data base backed up onto disc/tape/cloud at the end of each working day.

4.2.2: Where there is a need to transfer employee medical records to Fusion OH from a previous OH provider, Fusion Occupational Health Ltd will advise the client that:

- Employees must be informed of transfer
- Employees have the right to object to the transfer (in which case, the previous OH provider will need to be informed of the objections and retain control of the record unless a written request is received from the employees to have the record sent to them)
- All other medical records from current client employees will be transferred from the previous OH provider to Fusion OH at an agreed date and the relevant transfer of records document is signed and dated to acknowledge receipt of the records. This document should be scanned and saved within the OH shared drive.
- Employees who have left the client organisation within the last 6-year period will also have records transferred to Fusion OH. Health surveillance records for current employees and those that have left within the last 40 years will be transferred to Fusion OH as there is a legal obligation to hold these for 40 years.
- Where possible the previous OH provider should ensure a list of all records being transferred is provided to Fusion OH on the day of transfer.
- Fusion OH should check the records off against the list to ensure all are present.
- If there is no list received Fusion OH should catalogue all the records received and save the list on the shared drive. A copy of the list should be sent back to the previous OH provider and the client contact.

4.2.3: Where there is a need to transfer employee medical records to a new OH Provider from Fusion OH, Fusion Occupational Health Ltd will advise the client that:

- Employees must be informed of transfer
- Employees have the right to object to the transfer (in which case, Fusion OH provider will need to be informed of the objections and retain control of the record unless a written request is received from the employees to have the record sent to them)
- The agreed date of transfer of medical records and seek written agreement from the client for method of transfer e.g. encrypted disc send via special delivery.
- All other medical records for current employees will be transferred from Fusion OH to the new OH provider at an agreed date.
- Archive records for leavers that contain health surveillance records will be transferred from Fusion OH to the new OH provider at an agreed date, along with

general medical records for employees who have left the client company within the last 6 years.

- The relevant transfer of records document is signed and dated to acknowledge receipt of the records. This document should be scanned and saved within the OH shared drive.
- Where possible Fusion OH should ensure a list of all records being transferred is provided to the new OH Provider on the day of transfer.

4.2.4: Copies of any letters, reports, which are generated on an Occupational Health Professional's laptop, must always be filed within the individual's medical records either as hard copy, or scanned electronically to the designated server.

4.2.5: Data recorded and held must be:

- fairly and lawfully processed;
- processed for limited purposes;
- Patient-identifiable information only used if absolutely necessary;
- Use the minimum necessary patient-identifiable information
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in line with individual rights;
- secure; and, not transferred to countries without adequate protection.
- Restricted access, accessed only by those OH staff that need to have access.

4.3: Disclosure of any Information

4.3.1 Occupational Health staff including administrative staff must respect confidential information obtained in the course of professional practice or as a result of processing data and refrain from disclosing such information without the consent of the individual. Except where disclosure is required by law or by order of a court or if necessary in the public interest. In these circumstances the individual will also be informed.

4.3.2 Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In

this situation staff must discuss with the Clinical Director of Occupational Health or her deputy clinician and gain approval to disclose such information.

4.3.3 Occupational Health staff should inform the individual that a disclosure will be made in the public interest, even if you have not sought consent, unless to do so is impracticable, would put you or others at risk of serious harm, or would prejudice the purpose of the disclosure. Disclosure must be document in the individual's clinical record and include reasons for disclosing information without consent and any steps you have taken to seek the patient's consent, to inform them about the disclosure, or your reasons for not doing so. Occupational Health staff should also record who approved the disclosure.

4.3.4 Administration assistants must respect confidential information obtained in the course of their work and refrain from discussing or disclosing such information. This duty of confidentiality forms part of each Fusion employee's contract of employment.

4.4: Access to Medical Reports

4.4.1 Where the need for a medical opinion by a GP/Specialist/Other dealing with an individual is identified as part of the process of compiling a report giving clear, actionable, best practice and legislatively sound advice, the clinician must first explain the necessity for obtaining the report to the individual concerned.

4.4.2 The clinician must explain to the individual their rights under the Access to Medical Reports Act 1988, and ensure the client is given a copy of the principal rights (Access to Medical Records – on shared drive) under this piece of legislation.

4.4.3 The clinician must obtain the individual's written permission by completing the appropriate consent form (on the shared drive)

4.4.4 Once the individual's permission is obtained the clinician can request the medical report. The original signed consent form must be enclosed with the report request
and a copy held on file.

4.4.5 Where the report is required as a result of any of the following: - Post job offer health screening/Referral by Management. The clinician must ensure the Client Company designated person is aware of the request and that a time delay of 21 days is likely.

4.4.6 The clinician must ensure the individual is aware of any response that may be given to the Client Company designated person. The report must be filed in the individual's medical file.

4.4.7 Even if the individual does not exercise their right to see the report in advance the right of access remains for six months after its release without charge. However, under the Act health professionals may refuse access to information if it could:

- Cause serious harm to the physical or mental health or the individual who has asked for access, or to others

- Identify another, unless that third party consents, or is another health professional involved in the care of the patient

- Indicate the intentions of the practitioner in respect of the patient

These exceptions can apply to all or part of the report, but the employee must be informed as to whether access is being denied.

4.5: **Access To Health Records Act 1990 / General Data Protection Regulation/**

4.5.1 All requests for access to health records must be made in writing by the individual requesting access and contain signed/dated consent by the individual whom the records concern. The request will be forwarded to a member of the Clinical Governance (CG) Team for review.

4.5.2 OH professionals have ethical obligations around how patient records are shared, and where subject access requests are received from insurance companies the CG Team should explain to patients, in broad terms, the implications of making a subject access request so they can make a more informed decision on whether they wish to exercise their rights under the Data Protection Act. The CG Team should ensure they share any responses to subject access requests directly with patients/employees, rather than to insurance companies.

4.5.3 The individual's notes should be reviewed by a member of the CG team, to ensure none of the exclusions below apply: -

- In the opinion of the record holder, giving access would disclose information, which would seriously harm the physical or mental wellbeing of the person.

- In the opinion of the record holder, giving access would disclose information relating to or provided by an individual other than the person who could be identified from that information (unless the individual consents to disclosure).

- The relevant part of the record was written or complied before 1st November 1991 – except where disclosure of the records made prior to this date needs to be disclosed to enable the person to understand that part of the record to which access is required.

4.5.4 Once the designated clinician has reviewed the individual's notes, copies of the notes are to be sent to the individual concerned by special delivery, marked private and confidential and a record made of posting.

4.5.5 Access to the records is the decision of the Clinical Governance Team only and access If decided on, must be given within 40 days.

4.6: Disclosure of Information to Client Company

4.6.1 Where the nurse / doctor wishes to disclose clinical information to the individual's employer written consent must be obtained (on shared drive). This must be signed by the individual indicating that they agree to the information being relayed. The individual must understand

exactly what information needs to be released and should in most circumstances be privy to all relevant information, to whom, why, and the consequences of disclosure and non-disclosure.

4.6.2.1 Where an individual has indicated they would like to view the occupational health report before it is released to employer. They are made aware by the OH clinician that if they choose to respond to the contents of the report, they have up to 48 hours upon receipt by email to do so. They have up to 5 working days to respond if the report is posted. If no response is received within the stipulated timescales, the report will not be released and the referrer will be notified.

4.6.2.2 The individual can request that the clinician amend any factual inaccuracies but the opinion of the clinician cannot be amended. If the clinician is unable to amend the report, the individual will be notified and consent sought for the report to be released to the referrer with any comments supplied by the individual they want to be included.

4.6.2.3 The individual can withdraw consent at any stage should they wish to do so.

4.6.3 Where there is a need to transfer employee medical records to a new OH provider, Fusion Occupational Health Ltd will advise the client that:

- Employees must be informed of transfer
- Employees have the right to object to the transfer (in which case, Fusion OH will retain control of the record unless a written request is received from the employees to have the record sent to them)
- All other medical records will be transferred to the new provider at an agreed date by special delivery and the relevant transfer of records to a 3rd party document is signed and dated by the new provider & Fusion OH.
- Where possible Fusion OH should provide a list of all medical records being transferred to the new OH provider on the day of transfer.

4.6.4 All data protection incidents which breach legal or contractual requirements must be escalated to a Board Director. The Director in turn will co-ordinate an investigation and appropriate response. The incident will be reported to the Group Solicitor to identify any legal requirements and if required report to the company's insurers. The Director will also be responsible for notifying the Information Commissioner within 24hrs of the incident and notify affected individuals without undue delay. **See ISP-G-04 regarding management response to security incidents.**

4.7: Security of Documents Generated on a Laptop

4.7.1 The same basic principles that apply to manual records must be applied to computer held records.

- You are accountable for any entry you make in electronic-held records
- You must ensure that any entry you make is clear
- The identity of the person who made the record is clearly indicated
- The methods you use for recording information are secure

- The categories of staff who have access to records are clearly identified
- Procedures are in place to check whether a record is authentic when there is no written signature.

4.7.2 For medical records created and maintained on Fusion OH Ltd.'s Occupational Health Specific Server, no manual duplicates are required and hard copies scanned onto the server may be destroyed after 48 hours. The person responsible for scanning the hard copies onto the server, must ensure that all documents have been scanned by visually comparing the scanned document with the original hard copy.

4.7.3 Information generated on an individual Laptop or Tablet, should not be stored on these devices, but transferred to the Occupational Health Server as soon as is reasonably practicable.

4.7.4 The clinician must take reasonable steps to ensure that databases which are maintained for clients are up to date and backed up.

4.7.5 Where a clinician or others wish to terminate their employment with Fusion, their line manager should arrange for them to attend head office in person and hand over their laptop and other relevant electronic storage equipment, to a designated person who will check and log what items have been returned. This action is to ensure that all medical information is retained as confidential.

4.8 Retention of Medical Records

4.1 Medical records will be retained for all individuals who are currently employed by a Fusion OH client organisation. Medical records will also be retained for 6 years following notification an individual has left the client employment. Records produced as part of relevant legislation will be retained for 40 years following notification the individual has left the client employment.

4.2 Medical records (for leavers) that have been identified as reaching the above timeframe will be destroyed/deleted as per appropriate secure methods.

4.9 Mailing OH Records to Fusion OH Head Office from the Field Staff

4.9.1 Where there is a need to send hard copy records to Fusion Head Office for scanning onto Fusion OH System, The OHA/OHT will compile and photocopy all clinical documentation and complete a tracker with the description and list of documents included.

4.9.2 All documents are place in the courier bag or secure tagging envelop.

4.9.3 The OHA/OHT will contact the Fusion administration team to arrange collection and leave the package at the client reception for collection.

4.9.4 The OHA/OHT will email the enquires@fusionoh.com mailbox to confirm dispatch and confirmation should include:

- Date of dispatch
- Documents left at reception
- Description of documents in transit – including name of employee, Date of Birth and document name

4.9.5 Administrator on OH Queue to diarize expected date of package on post log.

4.9.6 Administrator to chase documents if not received within 3 working days of dispatch and escalate to line manager.

4.9.7 Admin to sign for documents in post book and update spreadsheet with document information and location including a list of the employee names and documents received. They must also check contents of package against tracker.

4.9.8 If any documents are found to be missing then this must be escalated to the line manager for further investigation.

4.9.9 On receipt of correct contents administration to forward documents for scanning on to shared drive.

4.9.10 Admin to check quality of scanned documents on shared drive and log onto post log to be checked for destroy date.

4.9.11 Admin to contact original internal sender to confirm documents are on shared drive and any hard copies destroyed.

5: Related Documents

Return to contents page

5.1: **Access To Health Records Act 1990**

5.2: General Data Protection Regulations come into force March 2018

5.3: Caldicott Report 2013

5.4: All other clinical/quality & information security procedures to be found in Fusion's policy/procedures folder on the shared drive

5.5: Fusion Process for OHA/OHTs Mailing OH Records