MANAGEMENT OF OCCUPATIONAL HEALTH RECORDS

1. PURPOSE

This procedure describes how medical records are stored, transferred, handled and accessed in the Occupational Health Service [OHS] at the University of Leeds.

2. SCOPE

Applies to all medical records in the OHS.

3. DEFINITIONS

Leaver's files are defined for the purposes of this procedure as any inactive files still held in the main data set where the data subjects are known to have left the organisation.

Archived files are defined for the purposes of this procedure as inactive files held separately in secure long term storage away from the main data set after the data subjects are known to have left the organisation.

Hard copy is defined as being all parts of a record written or printed.

Service is defined as another occupational health provider or representative, individual or body, of the patient to whom the records relate.

4. PROCEDURE

3.1 Records of current employees

The records of those working with current contracts will be retained in an accessible format in the service. This may be hard copy or electronic as part of Electronic Document Management (EDM).

3.2 Storage

The University of Leeds Head Of Occupational Health Service is responsible for ensuring security and confidentiality is adhered too. The department must be fitted with smoke alarms and filing space must be sufficient to meet current needs wherever reasonably possible.

3.2.1 Hard copy

All hard copy medical records are stored in locked metal cabinets with key access limited to as few members of the OHS team as necessary. All cabinets are locked out of office hours and the keys are stored in a secure area. The room containing the locked cabinets is also to be kept locked when unattended.

3.2.2 Non-paper storage

Reference Appendix 4.

- If any records are to be microfilmed, the person taking the copy must certify that the microfilmed copy is a true copy of the original record and signs and dates the copy.
- All non-paper confidential information must be kept in secure controlled locations, locked rooms, locked cabinets or security protected computer systems. All electronic health record information systems must have adequate logical and physical access controls with restriction to specific functions and/or data. Existing arrangements that are to be maintained for electronic data are as described under the table at the end of this document. Essentially all electronic data to be password protected. Where any electronic data is to be taken off campus by staff, data must be held on a high level encrypted memory stick.

3.3 Movement

Records or part thereof may be transferred/moved to another provider following the written permission of the individual to whom they relate.

3.3.1 Originals (or in the case of "part-work" contracts where the University of Leeds collects the data and sends it on to another provider, that part of the original attributable to the University of Leeds) must be fully copied before transfer to another Service and must be sent by recorded delivery using double envelope method. Inner envelope to be marked private and confidential and outer envelope addressed to addressee only. A register of records sent to another location is to be maintained.

3.3.2 Once the receiving service has received the original and have informed the sender of their safe arrival this is logged. The photocopy may be destroyed unless needed for other purposes.

3.3.3 When a photocopy document is sufficient, it is sent in preference to the original document e.g. complaints investigation, some legal requests.

3.3.4 Records **must not** be sent by facsimile.

3.3.5 All copies must by marked “COPY” on every page.

3.4 Register
Transfer of records to another service or department will be logged in a specific register for the purpose.

A register will contain the following minimum information:

- Employee full name and date of birth
- Employer (for whom the University of Leeds is working)
- Date of record movement
- New location name, address and phone number
- Purpose of movement (as above)
- Any additional information as required.

In the rare case of records being taken off-site by a member of staff additional information shall include:

- Reason for taking records
- Where records will be held
- How long they will be held (approximately)
- Signing that they will be held securely.

3.5 Missing records
This will be minimised by:

- Ensuring staff minimise the places where records may be kept
- Keeping a register of records transfers (e.g. sent to another location) to facilitate location.

A register of missing files with as much as possible of the information listed in 3.4 to be kept. Wherever records go missing the University's Information Security Officer must be immediately contacted and will take any necessary steps to minimise risk to those involved.

If a new set of medical records has to be made, this will be marked "Temporary File" and merged with the original when possible.

3.6 Retention of records

3.6.1 Records where legal cases are ongoing will be retained and identified "Retain – Required for Legal Purposes". Records may only be sent to archive once the case is **concluded, even if the employee has left the University of Leeds.**

3.6.2 Those records where there is a statutory requirement for record retention will be retained for the required period and so marked. They may be archived. If medical records are transferred to a new Occupational Health provider, a register (as above) is kept. Photocopies are made of the last two years to enable statutory returns to the HSE for Appointed Doctor work. (This is separate from any "health record" retained by the employer as required by law e.g. as in COSHH).

3.6.3 Data Protection Act 1998 – Period of retention.

Type of Data	**Maximum retention period**	**Reason for length of period**
Health Records	During employment	Management of Health & Safety at Work Regulations 1999
Records and reports relating to accidents	3 years after the date of the last entry.	Social Security [Claims & Payments] Regulations 1987; RIDDOR 2012
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years	Limitation period for personal injury claims. It may not be practical to separate from other aspects of Occupational Health records.
Occupational Health Medical records unrelated to a specific Health & Safety Regulation.	10 years after the end of employment.	Management of Health & Safety at Work regulations 1999
Medical records kept by reason of COSHH	40 years.	Control of Substances Hazardous to Health Regulations 2002
Ionising Radiation Records	At least 50 years after the last entry	Ionising Radiation Regulations 1999

3.7 Destruction of medical records

It is vital that confidentiality is maintained and that the method used to destroy such records secures their complete illegibility. Normally this will involve shredding, pulping or incineration.

When electronic archiving is undertaken the original medical records can be destroyed only after a written guarantee has been obtained that the records have been successfully copied into electronic format.

Non-paper records should only be destroyed in line with University policy and statutory and regulatory guidelines. It is vital that confidentiality is maintained at every stage.

3.8 Shared OH provision

Although not desirable, occasionally OHS will be involved in contracts where the University of Leeds is not the sole provider. At the start of the contact it must be made very clear as to who is the data controller and custodian of the records.

The University of Leeds can only be responsible for records generated by its staff. When individuals attend they must be informed that their notes may need to be moved between providers and the data controller will ensure a log of where records are stored is maintained.

The data controller must be approached for any access requests. If original records are requested from the University of Leeds as part of this process, administrators must copy those parts of the record that the University of Leeds has generated (in case of queries and subject access requests related only to university work) and store that copy. The movements of the notes must be logged.

3.9 Transfer of records from OHS to new Occupational Health provider

OHS will comply with transferring records to new Occupational Health providers on condition that:

- There are in place sufficient controls to guarantee the integrity of records is preserved and the Head of Service or an occupational physician, controls the process and is satisfied that the new provider has an identifiable clinical person who is responsible for the records.
- The records will be stored appropriately.
- The client has informed their employee(s) of the change of provider and individuals have had an opportunity to express their wish to have their records sent to their GP.
- Until transfer is complete, a case-by-case written consent system for records transfer may need to operate.
- OHS will be allowed access in case of claims.
- Charges for transfer of records may be levied to cover OHS costs.
- A register of records transferred and where they have been sent will be maintained to facilitate future enquiries.

3.9.1 Leavers files

Where the new provider is independent of management and has relevant professional qualifications then the records for past employees *may* be transferred to the new provider. Unlike for current employees, no specific consent is required.

In this way the totality of the occupational health records are kept in one place to the benefit of all employees – past and present.

3.10 Transfer of records to University of Leeds from another OH provider

Schools/other University services where an employee is based may request the notes from the previous/current provider with the consent of the individual to whom they relate. Arrangements for transfer should be discussed at the earliest opportunity. Employees have a right to request that the previous provider retain their records. Appendix 1 is an example of wording for request letters.

3.11 Access

The employee has right of access to their medical records under the Data Protection Act. All requests for access by patients shall be directed through an occupational health physician. Under no circumstances must administrators respond to requests for access to medical records made by the employee or his/her agents without reference to an Occupational Physician. In cases of doubt or when third party data is requested the Occupational Physician will consult with the appropriate person in the Secretariat.

3.11.1 Deceased Persons

OHS staff will release medical records about deceased persons in accordance with the Access to Health Records Act 1990 only upon receipt of a valid written consent from the next of kin or other *bona fide* authority with the advice of the Legal Department if required.

3.11.2 Access to medical records by other Third Parties

Employers are not allowed access to the content of records about employees but are entitled to copies of all correspondence with management regarding aspects of fitness to work relating to individuals and previously released. Employers are also entitled to check and audit storage facilities, provided medical confidentiality is maintained.

Exceptionally the process of ill-health retirement may require copies of the entire occupational health medical records to be sent to the Trustee appointed advisor. This will only be following the written consent of the individual, will be in unusual circumstances and only after an Occupational Physician has considered the circumstances.

In the event of medical emergencies e.g. an unconscious patient where OHS holds relevant medical information/records, these may be released upon the decision of a responsible Occupational Physician or their deputy using professional discretion.

Under the Data Protection Act it is also possible in exceptional circumstances to disclose medical records/medical information to third parties e.g.:-

- A Court Order requiring disclosure
- Suspicion of terrorism under anti-terrorism legislation
- Necessary to fulfil statutory obligations with regard to the protection of others e.g. DVLA Disclosure to the Police where failure to disclose would prejudice a criminal investigation.

These disclosures must only be made under the supervision of a responsible Occupational Physician and in many cases will not involve actual copies of records. The guidance of the General Medical Council will be followed.

Disclosure of medical records/medical information is also acceptable under for Notifiable Disease reporting and RIDDOR reporting. It is good practice to obtain the individual's consent for RIDDOR and Notifiable Disease reporting.

3.12 Confidentiality

Refer to the Appointments, reports, confidentiality and consent policy and procedure document.

All employees of the University of Leeds OHS, whether permanent or temporary must read the University of Leeds Confidentiality Agreement as applicable to Occupational Health. All employees must sign their understanding and agreement [Confidentiality agreement – *Appendix 2]*. It is the responsibility of Head of Service to ensure that staff are aware of the standards required and sign the form.

3.12.2 Reports may be sent by email to customers in exceptional circumstances provided that suitable security enhancing measures are used, including encryption. The details of the recipients email address must before transmission always be verified. In the absence of encryption and additional control at both the University of Leeds and the recipient end, password protection is regarded as suitable provided this is communicated separately.
(See Caldicott principles - *Appendix 3*).

3.13 Archives

As with current employee files, OHS should be satisfied that proper arrangements have been made if custodianship of archives is to transfer to a new provider. Each situation must be considered carefully and suitable arrangements made within the principle of maintaining integrity of the data set and subsequent ease of subject access if and when required.

If agreed within the contract and funded, as a general data protection principle it has been agreed with the Information Commissioner that the archived records of past employees *may* also be transferred to a provider. As with leavers' files, no specific consent would be required.

5. OUTCOMES & PERFORMANCE MEASURES

A decrease in errors and reduction in missing files identified by internal audit are to be the indicators.

6. REFERENCES & RELATED DOCUMENTS

University of Leeds Occupational Health Appointments, reports, confidentiality and consent document.
http://www.informationcommissioner.gov.uk/ Information Commissioners website
Access to Medical Reports Act 1988
Access to Health Records Act 1990
Data Protection Act 1998
Confidentiality. (General Medical Council)
Ethics guidance for Occupational Health Practice 2012. Faculty of Occupational Medicine
Fitness for Work: The Medical Aspects 4th Edition 2007 Palmer K, Cox RAF, Brown I. Oxford University Press.
Guidance on Records Management 2006 Department of Health
http://intranet.internal.leedsuniversity/occupationalhealth/htlm/workingguide/policiesprocedure
The Caldicott Principles (Caldicott Report December 1997) Common Law Duty and Confidentiality.

APPENDIX 1
UNIVERSITY OF LEEDS OCCUPATIONAL HEALTH SERVICE
Suggested form of Words for Individual Notes Transfer from previous provider

Dear

We have received a request from your employer to review your medical case and would like to arrange transfer of your Occupational Health medical records to ourselves as soon as possible.

If you are in agreement with the transfer of your records please sign and date the enclosed consent form and return it to us in the enclosed pre-paid envelope. We will then write to obtain the records.

If you do not agree to the transfer please contact Occupational Health Service at your earliest convenience.

Thank you for your help.

Yours sincerely,

APPENDIX 2

Occupational Health Service
University of Leeds
5-9 Willow Terrace
Road Leeds
LS2 9JT

Confidentiality agreement for staff

In the course of your employment or associated work in the Occupational Health Service, you may have access to, see or hear, confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals. On no account should such information be divulged or discussed except in the performance of your normal duties.

Breach of confidence, including the improper passing of computer data, will result in disciplinary action, which may lead to your dismissal.

You must ensure that all records, including computer screens and computer printouts of patient data, are never left in such a manner that unauthorised persons can obtain access to them. Computer screens must always be cleared when left unattended and you must ensure your computer screen is locked. All passwords to practice systems must be kept confidential.

No unauthorised use of the internet or email is allowed.

Information concerning patients or staff is strictly confidential and must not be disclosed to unauthorised persons. This obligation shall continue in perpetuity. Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the Data Protection Act 1998 or disciplinary action from the relevant professional body.

I have read, understand and agree to the terms and conditions set out above. I understand I will be required to read and sign this document on an annual basis whilst employed.

Signature ..... Date signed.....

Name (print) .....

APPENDIX 3

The Caldicott Principles

The Caldicott Committee established a number of principles aimed at improving the way sensitive patient data is handled

Principle 1 – Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 – Don't use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be used unless there is no alternative.

Principle 3 – Use the minimum necessary patient-identifiable information

Where use of patient-identifiable information is considered to be essential, each individual item or information should be justified with the aim of reducing identifiable.

Principle 4 – Access to patient-identifiable information should be on a strict need to know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

Principle 5 – Everyone should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Understand and comply with the law

Every use of patient-identifiable information must be lawful. A named person or nominee in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

APPENDIX 4

Occupational Health Service

Electronic Data Management

Electronic records containing patient personal data are held in the following places:

Spirotrac database (spirometry records only, identifiable by name)	Local PC	Located in Willow Terrace G03 & G04	Password is required to access the database server Password required to access the workstation (to access the file server)
Audiobase database (audiometry records only, identifiable by name)	\\occhlth5\ file server \\occhlth3\ file server (backup)	Located in Willow Terrace B.2	Password is required to access the file server(s) Password required to access the workstation (to access the file server) Password protection is available for the database but not implemented due to security on workstation/file server(s)
Documents (MS-Word, etc)	\\occhlth5\ file server \\occhlth3\ file server (backup)	Located in Willow Terrace B.2	Password is required to access the file server(s) Password required to access the workstation (to access the file server)
Documents (MS-Word, etc)	\\outlook.leeds.ac.uk\ Exchange server(s)	ISS network	Password is required to open the document(s). Emailed encrypted documents used for occasional communication with P/T Doctor
Documents (Dictation: Olympus, Dragon)	\\occhlth5\ file server \\occhlth3\ file server (backup)	Located in Willow Terrace B.2	Password is required to access the file server(s) Password required to access the workstation (to access the file server)

No patient or potential patient has any access to IT systems.