THE DEFENCE HEALTH RECORD

Introduction

1. Information is essential to the delivery of high quality evidence-based healthcare and health advice. Health records are a valuable and sensitive resource because of the information they contain. That information is only usable if it is correctly recorded, regularly updated, and easily accessible when required. The key security principles that underpin the handling of such records may be expressed as patient privacy, confidentiality, integrity and availability. These principles are to be converted into procedures by commanders responsible for Defence Health Records (DHR).

Background

2. Information is one of the four pillars[1] of the Defence Medical Services (DMS) Sub-Strategy and is essential in the delivery of core outputs:

a. Providing specialist medical advice on health and healthcare to the Chain of Command.

b. Delivering safe, effective, seamless, resource-efficient healthcare across Defence.

c. Developing and generating deployable medical capability; interoperable with our multi-national partners and capable in an increasingly complex mission space.

3. The military environment creates unique challenges for the maintenance of current, complete, accurate and accessible health records. Factors such as the transient nature of the population, dispersed locations of medical facilities, healthcare provision worldwide, the health information system and the mixed healthcare delivery model that uses DMS facilities, other military services facilities, the National Health Services (NHS) (including devolved administrations) and other service providers all contribute to this challenge.

Aim

4. The aim of this policy is to provide direction on the responsibilities associated with the DHR[2], in order to enable the DMS to achieve its core outputs.

5. This policy will contribute to the delivery of safe and effective patient care by maximising information accessibility to clinicians whilst meeting statutory and assurance requirements, and professional standards. It will allow information to be exploited whilst ensuring health information is adequately protected. It will emphasise the importance of record quality, making records readily identifiable, adherence to protocols to assist health information exploitation, and authority, responsibility, security and accountability for DHRs.

Scope

6. This policy addresses all health records created by the DMS and the creation, management, security, storage, handling, movement, archiving, retrieval, disclosure and disposal of DHRs and other sources of patient identifiable information.

Definition of a Health Record

[1] DMS Sub-Strategy Pillars: People, Patients, Partnerships and Information (P3I).
[2] Defined at Para 9.

7. A health record is any record or part thereof that consists of information relating to the health of an individual who can be identified from that information, or using additional information in the possession of the holder of the record. Such records will have been created by or on behalf of a health professional for the purpose of recording healthcare delivery. These include (but are not limited to) the following:

a. **Primary health care records.** This is the longitudinal Primary Health Care (PHC) record.

b. **Hospital patient records.** An episodic care record, specific to the place of care delivery.

c. **Occupational health records.** An episodic care record (e.g. a medical board, or an element of the PHC record).

d. **Admission and discharge, birth, controlled drugs and all other registers.** Health and healthcare registers which identify patients.

e. **Medical imaging and related reports.** The metadata which may be a physical folder with the image and the clinical report. This does not include anonymous images for medical training and education.

f. **Photographs and other images.** Not including anonymous images used for training.

g. **Laboratory samples and results.**

h. **Dental.** All forms of dental records, including dental casts[3].

i. **Medical equipment that holds information about healthcare provided and / or personal details.**

j. **Sexual health records.**

k. **Consent forms.**

l. **Aeromedical evacuation records.**

8. Health records can be on any media type, e.g. paper, CD, DVD, optical or magnetic, microfiche, audio, video, x-ray film, computerised i.e. emails etc.

Definition of the Defence Health Record

9. A DHR is the aggregation of an entitled person's[4] longitudinal PHC record and the records from any episodes of healthcare they have experienced whilst entitled. They include records from episodes of healthcare in a primary, secondary, tertiary or occupational setting, whether or not provided by DMS.

[3] This includes orthodontic casts.
[4] JSP 770 Triservice operational and nonoperational welfare policy. Chap 4.

10. There should be only one DHR per patient, and this is the spine to which the records of episodes of care should be attached. It is recognised that this is currently not the case and there is further work to minimise the number of DHRs to result in a single DHR for each individual.

Exploiting the Defence Health Record

11. The DMS is to ensure that the DHR resource is exploited. In doing so, due consideration is to be given to the following reasons for keeping and exploiting such records:

a. Duty of health professionals to maintain accurate, comprehensive and legible contemporaneous records of all healthcare encounters[5].

b. Meeting the expectations of the patient.

c. Optimisation of on-going healthcare.

d. Fulfilment of an individual's Terms of Service.

e. Essential part of healthcare governance.

f. Inform negligence claims.

g. Fulfilment of statutory obligations for the maintaining, storing, sharing and disposal of health records in accordance with JSP 441 Defence Records Management Policy and Procedures version 4, 2 Aug 11.

h. Support of Legal Justice (Lord Woolf) Reforms[6] that were brought in after a far reaching review and overhaul of the civil justice system.

i. Support of research, audit, teaching and accounting.

Principles for Defence Health Records

Statutory Requirements

12. There are numerous statutory and regulatory requirements that govern health records and these apply equally to all formats of records.

13. The legal principles that must be considered with regards to the DHR are contained in the following framework or legislations: Common Law Duty of Confidentiality, Data Protection Act 1998, Access to Medical Reports Act 1988 and Access to Health Records Act 1990. These legislations protect Patient Identifiable Data[7] (PID).

14. DMS personnel are responsible for the safe keeping of all patient identifiable information. Everyone working for or with the DMS who records, handles, stores, or otherwise comes across patient information, has a personal duty to comply with the Common Law Duty of Confidentiality.

[5] Paras 19-21, *Good Medical Practice – the duties of a doctor registered with the General Medical Council*, GMC, 25 Mar 13.
[6] Lord Woolf, Access to Justice, Final Report,http://www.dca.gov.uk/civil/final/overview.htm
[7] PID is defined as data that can be associated with an identifiable individual.

Common Law Duty of Confidentiality

15. The NHS Code of Confidentiality states, 'A duty of confidence arises when one person discloses information to another (e.g. patient to clinician, service user or carer to social worker) in circumstances where it is reasonable to expect that the information will be held in confidence.' The information includes that of patients, staff members, locums, temporary staff and anyone else's information that is held.

16. All DMS, contracted staff and locums must conform to this Duty of Confidentiality under the guidance or code provided by their own professional bodies.

Principles of the Data Protection Act 1998

17. The principles of the Data Protection Act should be upheld when dealing with any PID but is especially relevant with the storage of data within the DHR.

18. These principles in practice mean that individuals must:

a. Have legitimate grounds for recording, collecting and using PID.

b. Not use the data in ways that have unjustified adverse effects on the individuals concerned.

c. Be open and transparent about how the data is used, and give individuals appropriate privacy notices when collecting their PID.

d. Handle PID only in ways they would reasonably expect.

e. Make sure that the data is treated in accordance with the law.

Caldicott Principles

19. The Caldicott Principles apply to the handling of all health information to ensure the confidentiality of patients and service users is maintained as well as enabling appropriate information sharing in the interests of the patient. The principles are detailed below and in more detail at Department of Health Caldicott Guidance:

a. Principle 1. Justify the purpose(s) for using confidential information.

b. Principle 2. Don't use personal confidential data unless it is absolutely necessary.

c. Principle 3. Use the minimum necessary personal confidential data.

d. Principle 4. Access to personal confidential data should be on a strict need-to-know basis.

e. Principle 5. Everyone with access to personal confidential data should be aware of their responsibilities.

f. Principle 6. Comply with the law.

g. Principle 7. The duty to share information can be as important as the duty to protect patient confidentiality.

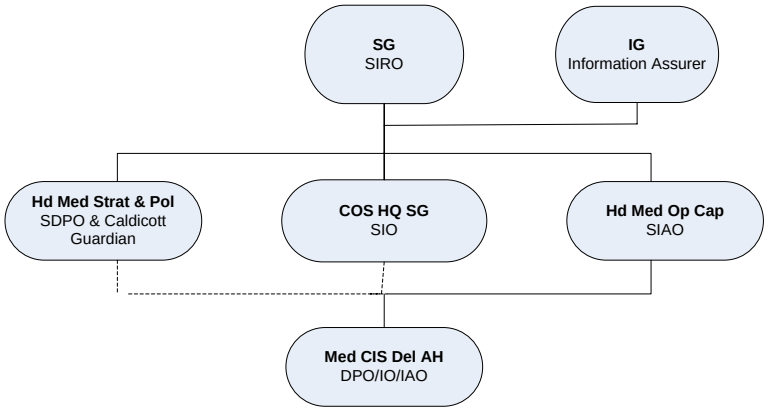
20. The DMS Caldicott Guardian is the Head of Medical Strategy and Policy, Headquarters Surgeon General. The post holder has executive responsibility for the management of healthcare records.

The Records Management: NHS Code of Practice

21. *Records Management: NHS Code of Practice*[8] has been published by the Department of Health as a guide to the minimum required standards of practice in the management of records by NHS organisations in England. It is based on legal requirements and professional best practice. These standards are to be followed within the DMS as a minimum requirement; although the retention periods required for DHRs are different and DMS retention periods will be published shortly. The DHR retention period ensures that it is retained for a minimum period for legal, operational, safety and research purposes and reflects the different business function of the MOD.

Responsibilities for Defence Health Records

22. Surgeon General (SG) is the professional head of the DMS and is the Process Owner for Defence Healthcare and Medical Operational capability. SG is responsible for assuring the quality of healthcare delivered to Service personnel and entitled patients, and for advising on the promotion and maintenance of health and prevention of injury and disease. These responsibilities include Senior Information Risk Owner for the DMS and overall accountability of DHR management. The following senior appointments are identified in support of DMS Information Governance Organisation:



Key:

DPO	Data Protection Officer – DPO
IAO	Information Asset Owner
IO	Information Officer
SDPO	Senior Data Protection Officer
SIAO	Senior Information Asset Owner
SIO	Senior Information Owner
SIRO	Senior Information Risk Owner

Protection of Defence Health Records

23. Anyone who has access to patient information is to observe patient confidentiality and avoid improper information handling in accordance with the principals outlined in the policy and in accordance with guidance or code provided by their own professional bodies.

Protective Marking of Healthcare Records

24. The classification of health records is mandated in JSP 440 Defence Manual of Security (Part 5, Section 2, Chapter 3), which should be read in conjunction with these instructions. As a general rule all patient identifiable records regardless of the type of document or whether it is paper,

[8] DoH (2006, 2nd Edition 2009). Records Management: NHS Code of Practice Part 2 (2nd Edition). http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

electronic, film or other media are to be protectively marked as PROTECT – MEDICAL: they are to be handled as if PROTECT – PERSONAL DATA.

25. The purpose of the protective marking PROTECT is to define a level of official information which needs to be protected from compromise of confidentiality, integrity and availability to a known level of assurance. PROTECT is a non-National Security Marking to safeguard information at Impact Level 1 and 2, the compromise of such assets (marked PROTECT) would be likely to:

a. Cause substantial distress to individuals.

b. Breach proper undertakings to maintain the confidence of information provided by third parties.

c. Breach statutory restrictions on the disclosure of information.

26. To ensure that the PROTECT marking is correctly applied across a wide range of material it is to be accompanied by a “descriptor”, for health records the descriptor is MEDICAL. Such descriptors are intended to reinforce the ‘need to know’ principle by showing the nature of the asset’s sensitivity. For a full list of descriptors, see JSP 440, Part 5, Section 2, Chapter 3, at Annex B.

27. Where disclosure of medical information is authorised (eg Joint Medical Employment Standards, functional limitations) this should be released under PROTECT STAFF, not PROTECT MEDICAL to avoid confusion.

28. Where information held is subject to an exemption to the access rights of individuals to their personal information, (for example, healthcare information which is considered detrimental to the health (mental or physical) of the patient) the documents are to be marked with NOT FOR DISCLOSURE TO PATIENT and not made available to the individual. If other exemptions apply, such as on grounds of national security, then NOT FOR DISCLOSURE markings are to be similarly applied.

Responsibility for Documentation of Healthcare Provision

29. DHRs are to be initiated, maintained and subsequently archived for all persons who receive care in a DMS or DMS contracted Medical Treatment Facility. It is the responsibility of the care providers to document the care delivered in order to ensure integrity of the DHR at all medical roles of care. The integrity of the record is to be maintained for all persons offered treatment, whether in the firm base or operational environment.

Ownership of the Health Records

30. The ownership of the information in health records lies with the organisation that has entered the information onto it. Hence, all information in the DHR entered by the DMS or DMS contracted service is the property of the Secretary of State for Defence. In practice MOD holds the records of its personnel ‘in trust’ on their behalf during their service. The patient may see that record at any time and is entitled to a copy of such information subject only to limited caveats[9].

[9] Data Protection Act 1998.

Creation of a Defence Health Record

31. The creation of the DHR is to occur on the occasion of the initial medical or dental appointment of an entitled person[10] at a DMS facility or DMS contracted facility. It occurs when the patient information is entered onto an electronic health record or paper record. This initiation will usually be when the entitled person's information is entered onto the Defence Integrated Electronic Health Record (iHR) or when an FMed 4, Personal Medical Folder or FMed 9, Hospital Record is initiated. The DHR continues to be added to throughout the period that the person is entitled to DMS care and treatment.

32. The iHR is provided for all serving members of the Armed Forces[11] and for eligible civilians (mainly Service families) whose healthcare is provided by the DMS in the Firm Base, deployed or overseas. The iHR encompasses the primary healthcare, dental and Occupational Health (OH) records. It also includes community specialist records for mental health and musculoskeletal rehabilitation for those personnel entitled to full DMS care. Those groups of personnel entitled to a more limited range of services such as OH provision only will also have an iHR.

Integration of health records from non-DMS sources to the Defence Health Record

33. There are circumstances where copies of health records from other organisations may be integrated into the DHR for example when an individual returns from an overseas posting where the provision of care is not delivered by DMS. The responsibility will be with the medical or dental centre that receives the records to integrate these into the DHR.

Entitled Patients who have NHS or devolved administration primary health records

34. When an entitled person's details are entered onto the Defence iHR and registered under a patient type that ends with [DMS], this indicates that the person is registering with a DMS facility and that the DMS is taking over the responsibility of the individual's Primary Healthcare. The presence of [DMS] at the end of the registration sends an electronic message that will initiate the de-registration of the individual from their General Medical Practitioner (GMP) and initiate the request for the paper NHS Primary Health Record (NHS PHR) to be sent to the Agency holding the Defence Records Contract (currently Lancashire and South Cumbria Agency, LaSCA).

35. A Regular service person's NHS PHR will be stored in the Agency's storage facility until the DMS parent Medical Centre requests the record or the patient is registered with a GMP on their transition out of the Services. If the parent Medical Centre requests the NHS PHR it will be sent directly to the medical centre for medical staff to gather the required information. The NHS PHR is to be returned to the Agency within 6 weeks of receipt. The service person's NHS PHR is not to have entries made into it during their service career.

36. A civilian DMS patient type (for example dependants who are registered at a military medical centre) will have their NHS PHR requested as for a service person, but on receipt the Agency will forward the record to the parent medical centre. During the provision of healthcare by DMS the clinical notes are to be entered onto the Defence iHR and also entered into the patient's NHS PHR.

37. Reserves when mobilised or FTRS (LC/HC) aircrew, Additional Duty Commitment aircrew and part time Reserve aircrew in flying appointments[12], and FTRS (Full Commitment), FTRS (LC/HC) appointed for service in Germany receive PHC from DMS and have the patient type

[10] The entitlement matrix for healthcare is in JSP 770 Chapter 4 and relates solely to overseas entitlements. There is ongoing work with HQ SG and Personnel to produce an equivalent, consolidated, list for the UK provision.
[11] Regular, and Reserve personnel.
[12] Entitled to full PHC on and off duty (AP 3392 Vol 7 Lftl 901 Annex A).

ending [DMS] on DMICP, and as such are processed in the same way as regular service personnel.

Entitled Patients with previous Defence Health Record

38. If a veteran (Regular or Reserve) becomes entitled to DMS Primary Healthcare their previous DHR is to be retrieved from the relevant archive. At their initial DMS medical appointment, the patient is to ensure that the medical staff are made aware they are a veteran. This will initiate a request by the medical staff (via the sS personnel records departments) for the Service person's previous DHR to be sent directly to the Medical Centre and their electronic recorded to be reactivated.

Entitled Patients with non-NHS or devolved administration health records

39. During recruitment, medical information or the health record may have been requested but this information is retained by the recruitment contractor and is not integrated into their DHR, nor stored at the Defence Agency. There are several groups in the Services[13] that come from countries where there may be no formalised healthcare system and hence they have no healthcare record created before they enter the Armed Forces.

Patients not entitled to primary healthcare

40. Primary Healthcare is not provided by the DMS for Reserves on FTRS Home Commitment (HC) or Limited Commitment (LC) who are not mobilised so they will remain registered with their own NHS GMP. For this reason, if these patient types are seen at a DMS establishment and they do not already have a iHR their patient type is entered as [Non-DMS], and so their NHS PHR is not called forward and remains with their GMP. Existing processes should be used to exchange information between doctors. Reservists should not be deregistered from the NHS GP as this may cause problems on their return and would be at a disadvantage as a result of service.

Maintenance of the Defence Health Record

The Defence Health Record in the Operational Environment

41. An Individual's DHR is to be delivered to, maintained and recovered from the Operational Environment in a seamless manner[14]. Accountability for the management and oversight of DHR in the Operational Environment rests with the nominated executive normally at Commander Medical, Commanding Officer or Officer Commanding levels. Specific guidance on the maintenance of the DHR in the Operational Environment can be found in the medical records chapter of the PJHQ J4Med Handbook on Joint Operations. Operational procedures are to be fully rehearsed by all deploying personnel, during pre-deployment training, to ensure that they are fully aware of their responsibilities in ensuring the integrity of the DHR in the operational environment.

42. Deploying medical personnel must be appropriately trained on deployed medical information systems such as DMICP deployed that will be utilised for the maintenance of the DHR in the operational environment.

[13] An example of such a group is Foreign and Commonwealth personnel.
[14] The Operational Environment is defined as any overseas employment of Defence forces commanded by Joint Forces Command or PJHQ excluding Permanent Joint Operating Bases, Overseas Bases and Contingency Operations. For operations within the UK mainland, overseas operations and exercises commanded by FLCs, these principles should also be applied. JDP 01 Campaigning 2nd edition.

The Defence Health Record in the Firm Base

43. The DHR in the Firm Base[15] is primarily reliant on the Defence iHR, currently provided by DMICP. The iHR has moved from the delivery phase to exploitation and an active effort is required to decrease the use of paper-based records within the DMS. DPHC and sS are tasked to reduce and hold a register of non-electronic practices.

The Defence Health Record for non-DMS overseas provision

44. In the majority of cases for patients taking up appointments overseas where the medical cover is non-DMS the DHR will be stored in accordance with JSP 950 10 -1-1 Healthcare advice for MOD Entitled Personnel and their Dependants posted overseas where there is no Defence Medical Services support. The patient must be made aware that if they have medical care provided in country that they must request a copy of their medical record and these are to be taken to their new medical centre on return. On receipt of the records they will be reviewed by a doctor and scanned into the iHR.

DMICP Portal

45. Correct management of the DHR in the Firm Base depends on formalised training on the correct management of the iHR and user compliance with the various process guides and protocols contained within the DMICP Portal. User manuals are available via the portal to inform and assist users and system administrators. The Portal is the sole repository for policy, processes and protocols approved by HQ SG.

46. It is essential that the medical chain of command make individuals aware of changes that might impact on them, and ensure adequate training is made available as part of the implementation of business changes. It is the responsibility of individuals to make themselves aware of the content of information sources to which they have been directed, or of training which is delivered to them.

Paper Records

47. FMeds are to be used to record patient information when the iHR is unavailable. It is the responsibility of the person entering information on the FMeds to ensure that whenever possible it is the official and most up to date version of the form that is being used. The use of unauthorised or locally amended FMeds is not permitted. HQ SG Strat Pol is responsible for ensuring that the FMeds system is flexible, responsive to changes in the clinical and operational environment and fit for purpose. The contact for information on FMeds and proposed changes is SG ACDS StratPol-Nursing SO2.

Scanning

48. In order to comply with the Code of Practice for Legal Admissibility and Evidential Weight of Information, documents are to be scanned at a minimum of 300dpi resolution. Higher resolution will utilise more digital storage or memory space, but scanning at 600dpi or higher should be considered where originals are smaller than B6 (postcard) size, or where other factors (such as faded or difficult to read handwriting) indicate that a higher resolution is required. To comply with the Code of Practice, image manipulation processes, such as de-speckle, de-skew and cropping, are not permitted. This ensures the integrity of the image.

[15] Firm Base refers to where an expeditionary Armed Force can be suitably quartered, prepared and trained, and from which it can be readily detached and supported.

49. Units are to undertake their own scanning; however such scanning must comply with 2013DIN05-021 and is subject to audit by CIO. The scanners supplied to medical and dental treatment facilities are 300dpi resolution. This resolution is not sufficient for ECGs, spirometry and audios and appropriate arrangements need to be made so they are scanned at high resolution to keep them readable post scanning. If scanning is to be outsourced, this work is to be placed through DBS KI-Records with the MOD contractor, currently TNT.

Scan and shred

50. Medical and dental staff are to take a pragmatic 'scan & shred' approach to ensure a 'paper-light' approach to the DHR. Scanning onto the iHR ensures that the iHR contains all relevant information and minimises the requirement to maintain paper-based medical records such as the FMed 4. In the unusual circumstances where the iHR is not available, it may be necessary to maintain paper-based records.

51. Retaining original copies of documents in the paper DHR that have been scanned onto the iHR is unnecessary. Once information is scanned into the iHR and it is checked that it is of a sufficient quality to be readable and the system has had an appropriate period of time to synchronise with the main server (48 hours) original copies of documents must be shredded. Navy Service Medical Board of Survey records documentation should not be shredded in accordance with BR1991[16].

Temporary National Health Service Registration

52. A patient registered with the DMS for primary healthcare will be unable to register with an NHS doctor for the long term provision of their primary healthcare, although they will be able to access NHS primary healthcare as a 'Temporary Resident' for a maximum of 3 months. Those personnel registered as '[DMS]' patients that visit an NHS medical or dental facility and register as a temporary resident will have health records made for that consultation. These records will be forwarded to LaSCA and then onto their registered medical centre for integration into their DHR or in the case of dependants into their NHS PHR. All health care records are to be seen by a doctor or practice nurse and any follow up action recorded and undertaken.

53. The converse is possible, where an individual is treated by DMS under the equivalent of temporary registration provisions, for example if a child who is normally registered with an NHS GP as he/she is at boarding school, is treated whilst on holiday in Germany visiting his/her parents, the DMS medical centre should follow the process in reverse and send the notes pertaining to the treatment to LaSCA, for onward direction to the child's NHS GP.

Health Records for integration into an existing Defence Health Record

54. There will be situations after the DHR has been created when the individual may be seen by a non-DMS provider e.g. temporary NHS registration or overseas. In these cases the clinical records are to be sent to their registered DMS practice and given to the practice nurse or doctor to assess significance, ensure follow up procedures and summarise as appropriate onto DMICP. Paper records are to be scanned into the iHR and shredded (see Para 51). Electronic records are to be integrated into the iHR and original electronic copies destroyed.

Patient identifying information

55. It is essential to link patients with their health records. The patient identifying information is to be sufficient and unique to ensure that records can be retrieved irrespective of elapsed time. All

[16] BRd 19919 Chap 8 Articles 08169g) and 0824.

correspondence with the NHS in England and Wales must include the patient's unique NHS Number. All correspondence with NHS Scotland must include the patient's unique Community Health Infox (CHI) number.

Non-electronic Defence Health Record storage

56. Current records are to be kept in a location where they can be easily recovered when required. They are to be stored alphabetically and secured in lockable fire-proof drawers or cabinets, within rooms that are to be locked when left unattended.

Access to healthcare workers documents by members of staff

57. There is the possibility of an ethical conflict if an individual's treating clinician is also their line manager. To eliminate this ethical conflict, military primary healthcare staff can, if they choose receive their healthcare from another medical centre other than that which they work in. It is appreciated that this is not always possible. To minimise the risk of inappropriate access to or release of personal and medical information relating to medical staff, paper records are to be held in a separate locked drawer and the keys held by the Practice Manager, Senior Medical Officer or Senior Nurse. Staff iHRs are only be accessed by a treating clinician or on their direction (e.g. direction to a pharmacy technician in the form of a prescription).

58. All DMS practices must implement an effective audit process to ensure that staff records are regularly assessed to detect any illegitimate access by non-authorised members of the practice team.

Request for access to Health Records

59. For an individual to request a copy of their DHR a Subject Access Request (SAR) form needs to be completed and forwarded to the Practice Manager in accordance with the DPA 1998. This JSP includes copies of the form and details of the process.

60. Guidance about a request from a solicitor for medical information can be found in JSP 950 1-2-9.

Defence Health Record on leaving

61. On discharge the patient is to be given a paper FMed 133 (Medical History on Release from HM Forces) that includes information on vaccinations, medicals and a summary of their healthcare. They are to be advised to take this form to their NHS General Practice on registering. On registering with an NHS practice there will be an automated request for the NHS PHR held at LaSCA. Copies of the DHR will be available to the NHS practice if they require them, following the guidance on the FMed 133.

Movement of Defence Health Record

Movement and transportation of paper healthcare records

62. The process for the movement and transmission of health records is mandated in JSP 440 Defence Manual of Security (Part 5, Section 3, Chapter 1) and JSP 367 Defence Postal and Courier Services (Chapter 4, paragraph 14). The relevant instructions have been extracted from these publication and are captured in the sections below.

Packaging of physical healthcare records

63. Whenever health records are moved or sent outside of a practice, the documents are to be double wrapped. A RAF Form 591 is to be enclosed inside the inner envelope with the health records. On the inner envelope an FMed 180 Gummed Transit Label is to be attached and the protective marking (i.e. PROTECT – MEDICAL) is to be used. The protective marking must not be visible from the outer cover, packaging or container. Window, transit or self-sealing envelopes are not to be used as they cannot protect information from unauthorised viewing.

64. The outer packaging is to have a return address, to which replies, receipts or other correspondence can be sent. In other words, health records anywhere outside the purely electronic environment are to be treated as if they were protectively marked “SECRET”, which the method described here ensures. Taking this action minimises the likelihood of losses.

Postage of paper records in UK and using Defence Courier Services

65. DHRs are to be sent as ‘Special Delivery’. The use of ‘Special Delivery’ will ensure there is proof of posting and delivery, and also provide a fully traceable service that ensures the items are signed for at each stage of the process. This provides an enhanced level of traceability in the event of loss. The cost of utilising this service will be borne by the Defence Mail Centre (DMC). Units not served by a DMC will be responsible for their own costs[17].

66. The only exception to the use of ‘Special Delivery’ for DHR is when over 50 DHRs are being returned from Operational Theatres. In this case, DHRs are to be packed and indexed into one package and escorted by the Defence Courier Service as a Special Move item.

Postage of paper records from or to units based in other NATO countries

67. All NATO countries are bound by STANAG 2109 (EN-Postal Organization and Courier Service) for the NATO Forces which requires items not to be opened by member country customs officials even when not protected by diplomatic cover. Therefore, units based in other NATO countries or sending items that will only pass through other NATO countries are to ensure that the items are carried in accordance with STANAG 2109.

68. As instructed in STANAG 2109, when movement of PROTECT – MEDICAL assets has been approved, the consignor is to instruct the shipper to prepare a Notice of Movement. This should give:

a. Details of the assets.

b. Means of transportation.

c. Date on which the assets will leave the consignor.

d. Estimated date on which the assets will arrive with the consignee.

69. Copies of the Notice of Movement are to be sent to the consignee in time for them to make adequate security arrangements at the delivery point. The Notice of Movement itself should not be protectively marked and should not contain any protectively marked information.

[17] JSP 367, Defence Postal and Courier Services, chapter 4, paragraph 14.

Receipting of paper records

70. Receipts are to be included when packaging and sending medical notes. An RAF F591 'Receipt for Personal Documents' must be used, as it receipts both dispatch and arrival of documents. When delivery is hand-to-hand, a MOD Form 32, Receipt for Documents is to be used. In all cases, the receipt is to provide the following:

a. The sender's (consignor) full postal address – to which the receipt is to be returned.

b. Details of the documents sent (an inventory) – typically the patient's name, date of birth, Service or Hospital Number, document type (e.g. FMed 4).

c. Details confirming receipt – an area set aside for the signature, name (in block capitals) and address (branch stamp if available) of the person who opens the envelope or package.

Removable media

71. In accordance with JSP 440 Defence Manual of Security, patient identifiable health records are to be classified as PROTECT – MEDICAL with an impact level of IL1-2. Therefore, if it is necessary to copy such records to removable media (CD-R etc) then colour coded media must be used (See JSP 440, 5-2 Para 38). These are special order only; each disk has a unique serial number and is an accountable asset, even when blank. The colour for PROTECT – MEDICAL / PERSONAL DATA is buff.

Electronic transmission of PROTECT – MEDICAL information

72. Information marked PROTECT – MEDICAL may be transmitted across the internet / in e-mail without encryption, providing the personal data being sent belongs to the individual sending it i.e. the owner of the medical record.

73. There is a dedicated email gateway between the MOD RLI and NHS N3 network, which allows the secure transmission of email classified up to and including RESTRICTED material. When emailing a person with an email address ending @nhs.net, this will be sent over the secure gateway and can be used, with the appropriate markings, to send patient confidential information. NHS email accounts which end with any other domain address for example @trustinengland.nhs.uk are not secure and must not be used to send information other than UNRESTRICTED.

74. If neither of the conditions above are met then data marked PROTECT – MEDICAL may be transmitted across the internet (i.e. by email), but is to be encrypted using standard commercial products. The commercial products must meet the FIPS 140[18] standard as a minimum. Local Information Security Officers are to be consulted for advice on encryption products. If encryption is unachievable or the delay in implementing such measures may cause harm to the patient then it may be sent without encryption, however the medical data is to be sent separately to the personal information to minimise the risk of compromise. Transmissions without encryption may be subject to audit and there will be a requirement to justify why the normal secure methods of transfer were not used.

[18] The 140 series of Federal Information Processing Standards (FIPS) are U.S. government computer security standards that specify requirements for cryptography modules.

Legal admissibility of electronic records

75. The term “legal admissibility” is commonly used to describe the likelihood that evidence presented during a court case will be accepted. In some cases, the relevance, correctness or completeness of clinical notes may be challenged. The Defence iHR is designed to ensure that there is an electronic trail for each key stroke and this together with the secure log-in details is admissible to replace a clinician’s signature on medical documents.

Archiving and retaining Defence Health Records

Central Health Records Library service

76. The purpose of the Central Health Records Library (CHRL) is to provide a high quality, safe central repository for medical and dental records[19] of MOD origin to support the healthcare of HM Armed Forces. In doing so, CHRL shall:

a. Provide a safe and secure storage facility.

b. Retrieve, handle and release copies of health records in accordance with applicable legislation.

c. Provide support to the DMS, NHS and other healthcare providers, in their provision of ongoing care to patients.

d. Provide support to MOD in its assessment of litigation cases.

e. Provide support to Service Pensions and Veteran’s Agency (SPVA) in their assessment of claims and provision of Pensions and Compensation payments.

f. Reconstruct primary healthcare records (where possible) from discrete records when unit medical centres, Medical Boards or single Service personnel branches are unable to locate the original FMed 4 folder.

g. As required provide copies of personal medical records to individuals (the patient) in response to SAR in compliance with DPA 98.

h. Maintain patient confidentiality.

i. Deliver transparency, efficiency and value for money.

Procedure for movement of large numbers of documents

77. Units that are closing or drawing down, particularly those units overseas that require information on the process of DHR transportation and disposal, are to contact CHRL or if related to operations to contact PJHQ.

Depositing records with CHRL

78. When sending large quantities of healthcare records to CHRL, these must be indexed, boxed securely and packaged as detailed below. The maximum weight for each box is not to exceed

[19] This archive facility for dental records should include appropriate storage of dental / orthodontic casts or scanning and archiving of the casts itself or in the form of a 3D image as an alternative.

10kg. If necessary, these boxes can be placed inside larger boxes that can then be bound or wrapped together for palletising.

79. Two copies of an inventory list are to be created for the contents of each box. One copy is to be sent ahead to CHRL (by post, fax, or email if via RLI / DII) the other placed inside the appropriate box.

80. When possible, the advance copy of the inventory list is to be emailed to CHRL. Providing the list contains less than 1,000 patient's names it can be sent via email without encryption.

81. Consignments consisting of more than one box are to be labelled to show the total number of boxes being sent and the date of posting.

82. The boxes and inventory lists are to be sent with a covering letter giving full contact details of the sending unit. The consignor is to liaise directly with CHRL before dispatch so that due provision of resources and space is available for receipt of the delivery. A copy of the Notice of Movement is to be sent to CHRL (by email or fax) to confirm the expected delivery date, in time for adequate security arrangements at the delivery point.

83. Health records are to be sent to:

The Central Health Records Library
Room 24
Sentinel House (Building B1)
MOD Shoeburyness
Southend-on-Sea
Essex, SS3 9SR

SG ACDS MedOpCap-MedIS-CHRL Requ (MULTIUSER)

Main Office Number 01702 299310
Facsimile 01702 294702

Archiving of sexual Health Records at CHRL

84. In accordance with best practice, sexual health records are to be stored at CHRL with 3 patient identifiers including name, date of birth and clinic number. Notes are to be boxed with a list of the contents of each box. The list is to be stored centrally by the Military Advice for Sexual Health hub at Birmingham Heartlands Hospital. If access is required to patient notes, specific written patient consent to access genitourinary notes is required and this is to be included on the SAR Form.

Requests for the retrieval of records

85. Requests for the retrieval of health records is to be made to:

The Central Health Records Library
Room 24
Sentinel House (Building B1)
MOD Shoeburyness
Southend-on-Sea
Essex, SS3 9SR

SG ACDS MedOpCap-MedIS-CHRL Requ (MULTIUSER)

Request Team Hotline	01702 299300
Facsimile	01702 294702

86. Although telephone enquiries are permitted, it should be noted that health records will not be released without a formal written request first being received by CHRL.

87. Formal written requests for healthcare records are to include as much information as possible regarding the patient's identity, the hospital or facility where the treatment was provided and the treatment date.

Archiving the Defence IHR

88. The Defence iHR is to remain active for a year after the individual leaves the Service or loses their entitlement to DMS services. An archiving policy is being developed.

Disposal of records

89. Regular review and disposal of records is to be considered in accordance with the guidance on the length of retention of records that will be added as an annex by Jan 14. If applicable, written records and associated paper documentation can be destroyed by medical staff. A list of notes to be destroyed is to be produced, noting patient surname, given name, date of birth, service number and gender. A register of all destroyed notes is to be kept either electronically or on paper which is to be stored securely.

90. Notes are to be shredded within the medical clinic then incinerated. Any shredder is suitable for this purpose. This process is to be undertaken by at least one member of staff witnessed by a second member or a person nominated by the Caldicott Guardian. The process is to be confirmed by visual inspection that the shredded waste is thoroughly incinerated.

91. The MOD has confidential waste contracts, which may be used for this purpose and these services can be accessed via local level or if a contract is required refer to 2013DIN04-006 Closed loop secure document destruction and waste paper management and recycling.

MOD publications with references to Defence Health Record management

92. This JSP 950 contains the relevant information from the documents mentioned above. If more detail is required reference should be made to JSP 375 MOD Health and Safety Handbook Vol 2 April 2010 Leaflet 55 and JSP 441 Defence Records Management Policy and Procedures.

Implementation

93. Unless cancelled or otherwise revised, this leaflet is to be routinely reviewed after five years. HQ SG is to make policy leaflets publicly available in accordance with the Freedom of Information Act. This policy leaflet is releasable to the Internet. An Equality Analysis has been undertaken in the production of this policy and no impact is anticipated in terms of the Equality Act 2010.

Authorisation

94. This policy is released for publication by Head of Medical Strategy and Policy on behalf of the SG.

Point of contact

95. Point of contact is SO2 Medical Policy at HQ SG, via email SGACDSStratPol-MedPolSO2@mod.uk or by telephone on 01543 434669.