NHS
Halton
Clinical Commissioning Group

EMIS to EMIS

Patient Record Data Sharing

CONTENTS

1. Policy Statements and Purpose of this Data Sharing Agreement 3

2. Legal Basis for Data Sharing 4

3. Data 4

3.1 What data is it necessary to share? 4

3.2 Who is going to be responsible for sharing this data and ensuring data is accurate? 5

3.3 How will you keep a record of what data has been shared? 5

3.4 How is this data going to be shared? 6

3.5 Who will have access to this data and what may they use it for? 6

3.6 Timescales 7

3.7 How securely does the data need to be stored? 7

3.8 How long are you going to keep the data? 7

3.9 Further Use of Data 8

4. Breach of confidentiality 8

5. Complaints procedures 8

6. Access to Information 9

7. Indemnity 9

8. Review of Data Sharing Agreement 10

9. Closure/termination of agreement 10

10. Signatories 10

1. POLICY STATEMENTS AND PURPOSE OF THIS DATA SHARING AGREEMENT

This purpose of this data sharing agreement is to underpin the sharing of clinical patient information within EMIS Web with the aim of supporting direct care delivery. The shared record will be available to support the care management of patients within various health and social care services across Halton and therefore accessed by staff who have a legitimate relationship with the patient they are caring for.

The aim is that this data sharing agreement will supersede previous multiple data sharing agreements and provide one over-arching agreement centred around the same principles and processes that all partners utilising an EMIS Web system will adhere too. As such, the below organisations are aligned to this data sharing agreement and will be either viewing or sharing clinical information (or both).

Organisation	Viewing (Data Processing)	Sharing (Data Controller)
NHS Halton CCG Member Practices (14)	Yes	Yes
Bridgewater Community NHS Foundation Trust	Yes	Yes
Warrington and Halton Hospitals NHS Foundation Trust	Yes	Yes
Halton Haven Hospice	Yes	Yes
GP Health Connect	Yes	Yes
Widnes Highfield Health	Yes	Yes
Halton Borough Council	Yes	No
NHS Halton CCG	No	No

The agreement will underpin the data sharing technical functionality within EMIS and provide the principles and basis for accessing the shared data. The data sharing functionality within EMIS provides a 'shared record view'. This provides only a view of the shared information and the information cannot be added to/or amended within a sharing partners host system.

If a shared record is available this will be highlighted in a clickable tab alongside the patients’ clinical record. If the reviewing staff member requires additional information that may be available within a shared record, they will be able to click the shared record tab. The staff member can then search on a specific code or view a recent investigation etc. as relevant and pertinent to the consultation.

2. LEGAL BASIS FOR DATA SHARING

This Data Sharing Agreement has been developed to achieve the objectives as set out in Section 1. It is the intention that all aspects of information sharing and disclosure relating to this agreement shall comply with legislation that protects personal data.

The lawful basis to exchange this data is direct care. Each of the organisations listed within the agreement are commissioned to provide services for Halton residents. Staff members employed within these organisations are provided access to the clinical system relevant to their role and as such have a legitimate relationship with the patients that they are providing care to.

3. DATA

3.1 WHAT DATA IS IT NECESSARY TO SHARE?

The data being accessed as part of this agreement is related to the care management of an individual patient who has a legitimate relationship with the viewing staff member for direct care delivery. For example, if a patient attends a community appointment, the assessing clinician will access the record for that individual patient to inform and support the consultation being undertaken. As such the data needs to be identifiable as it is linked to the patient who has attended the service.

The shared record view makes all data within a clinical record accessible to the requestor except for a number of sensitive data items which have been excluded from this data sharing agreement. A list of these codes has been provided in Appendix 2. The excluded codes will not be made available within the shared view and will only be available within the local system if they have been recorded.

The requestor will be based within an organisation that has a legitimate relationship with the patient and will be accessing the shared information to support direct care delivery. Clinicians will be expected to search within the record only for the information that is pertinent to the episode of care.

All Parties should ensure that their Fair Processing Notice, which should be publicly available, provides detail of the data being shared as part of this agreement and its purpose.

3.2 WHO IS GOING TO BE RESPONSIBLE FOR SHARING THIS DATA AND ENSURING DATA IS ACCURATE?

The data that will be shared is the data that has been recorded locally within the host system in relation to a patients' episode of care. This information is deemed to be an accurate record of the care that has been provided to the patient in line with local record keeping policies. There is no other requirement for an individual to physically share information as this will automatically be available via the EMIS shared record under the legal basis of direct care.

The data will be available within the EMIS Web clinical system and therefore will be viewable in the same format as the host system and will be reflective of the clinical templates that have been built to support the service. The viewing individual will be expected to identify the information within the shared record that is relevant to the episode of care.

Any inaccuracies that have been identified are the responsibility of the host organisations to address and where appropriate the viewing organisation should alert the host organisation to the error.

3.3 HOW WILL YOU KEEP A RECORD OF WHAT DATA HAS BEEN SHARED?

All data held within a patients clinical record (except the exclusion codes listed in Appendix 2) will be available as part of the shared record. As such, organisations should ensure that all staff are aware that this is the case and that information should be recorded in an appropriate manner and acknowledge that all information will be made available to the parties listed in Section 1 at a level that is appropriate to their role.

All user actions within the system are fully auditable therefore along with auditing when a shared record has been accessed, actions within the shared record are also auditable by user for example if a specific code is searched within the shared record or a document has been accessed.

3.4 HOW IS THIS DATA GOING TO BE SHARED?

Data will be shared via the EMIS Web clinical system. If a shared record is available for a patient i.e. the patient has attended another service and information has been recorded on their record a shared record view will be available to all EMIS sites.

If there is any interruption to the shared record functionality and access to local records is still available, clinicians should continue to adhere to relevant record keeping policies and resume access to the shared record once this access has been restored within the system.

3.5 WHO WILL HAVE ACCESS TO THIS DATA AND WHAT MAY THEY USE IT FOR?

The data will be available for clinicians and staff in commissioned services that are delivering direct care to patients. This will include staff within both health and social care services within the organisations listed in Section 1.

Each organisation will be responsible for ensuring that starter and leaver policies are adhered to. This will include ensuring that new users are provided with access to clinical systems that are appropriate to their role and also ensuring that any staff members who leave the organisation are archived within the clinical system.

As part of the induction process, all organisations listed should ensure that staff are aware of the shared record availability and the policies and procedures outlined within this data sharing agreement. Any local confidentiality policies relating to this agreement should also be followed.

3.6 TIMESCALES

It is expected that the shared record will be accessed as required for the care management of the patient. The record should only be accessed in relation to a direct care purpose and should not be accessed if the patient has never been known to a service or if there is no clinically appropriate reason to do so as this patient should not be registered with the service. There is no specified time limit associated with this agreement and the care record information will be available to services for the duration of the patients' lifetime (or life of the clinical system) if required.

3.7 HOW SECURELY DOES THE DATA NEED TO BE STORED?

As no data is being physically transferred as part of this data sharing agreement, data will remain in the host EMIS system which is hosted on a secure N3 connection within the European Economic Area. A read only view of data is provided by the shared record access but no data is transferred into the viewing system.

Each user is to be provided with a secure login based on their role within the organisation to access the clinical system. For example, a GP should be assigned to a GP role within the EMIS clinical system. All the data included within this data sharing agreement will be electronic and therefore there will be no requirement to store paper records. All users should adhere to policies in relation to clear screen/desk and should ensure they have logged out of the system when leaving their office building.

Data should only be accessed by those individuals that have a legitimate relationship with the patient.

If there is a security breach in which data received from another party under this agreement is compromised, the originator will be notified at the earliest opportunity.

3.8 HOW LONG ARE YOU GOING TO KEEP THE DATA?

Within the EMIS Web Clinical System there is no functionality to permanently delete a clinical record. As such the archiving functionality should be utilised in line with the NHS Records Management Code of Practice. The below standards relevant to this agreement have been included in Appendix 3. The full document can also be accessed at the flowing link: https://digital.nhs.uk/codes-of-practice-handling-information. The retention of data is only applicable to the data controller and no data is extracted as part of this data sharing agreement.

3.9 FURTHER USE OF DATA

The data referenced within this data sharing agreement, will only be used for the purpose specified and will not be used for any other purpose.

If a Party to this agreement wishes to further share the information they should contact the CCG.

4. BREACH OF CONFIDENTIALITY

Partners aligned to this agreement should follow their own policies in relation to security breach/breach of confidentiality and the CCG/other parties should be kept informed/involved as appropriate

Should the breach involve a member of staff, a full audit should be undertaken by the breaching organisation to identify the member of staff including detail of how the breach took place. This should be undertaken by the identified governance lead within each organisation listed. An action plan should then be presented to the commissioning lead detailing mitigating actions that can be put in place. Any breaches must then be dealt with in line with organisational disciplinary policies.

5. COMPLAINTS PROCEDURES

Patients have been provided with details of the CCG Complaints process as part of CCG literature and this information should also be accessible via organisational websites. The CCG will engage with parties if a complaint is received to investigate further. If a complaint in relation to the service or data sharing is notified to Parties direct, the CCG should be notified and support services to coordinate a response as per current complaints processes.

6. ACCESS TO INFORMATION

All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 1998. While there is no requirement to consult with third parties under FOIA, the parties to this agreement will consult the party from whom the data originated and will consider their views to inform the decision making process. All decisions to disclose must be recorded by the disclosing organisation.

Each Partner Organisation shall publish this agreement on its website and refer to it within its Publication Scheme. If a Partner Organisation wishes to withhold all or part of the agreement from publication it shall inform the other Partner Organisations as soon as reasonably possible. Partner Organisations shall then endeavour to reach a collective decision as to whether information is to be withheld from publication or not. Information shall only be withheld where, should an application for that information be made under FOIA 2000 it is likely that the information would be exempt from disclosure and the public interest lie in favour of withholding. However, nothing in this paragraph shall prevent the individual Partner Organisations from exercising its obligations and responsibilities under FOIA 2000 as it sees fit.

The sixth principle of the Data Protection Act 1998 provides individuals the right to have access to information held about them with limited exemptions. It is necessary to ensure that only appropriate access to information is granted therefore the agreement must detail the responsibilities of each organisation to ensure individuals rights are met appropriately. The Freedom of Information (FOI) Act (2000) gives everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

7. INDEMNITY

Each partner will keep the Data Controller fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner, of any data obtained in connection with this agreement.

8. REVIEW OF DATA SHARING AGREEMENT

This agreement will be reviewed annually, engaging with all organisations identified in Section 1. This will then be formally noted via the Information Management and Technology (IM&T) Working Group and any required amendments recorded and an updated version recirculated to all organisations for review.

9. CLOSURE/TERMINATION OF AGREEMENT

Any partner organisation can suspend this agreement for 45 days if security has been seriously breached. This should be in writing and be evidenced.

Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the signatories of this agreement, or their nominated representative. This meeting to take place within 14 days of any suspension.

Termination of this Data Sharing Agreement should be in writing to all other Partner Organisations giving at least 30 days' notice.

10. SIGNATORIES

The signatory within each of the below organisations should be the person responsible for data protection within that organisation.

Signatories:

- NHS Halton CCG
- NHS Halton CCG Member Practices (14)
- Bridgewater Community NHS Foundation Trust
- Warrington and Halton Hospitals NHS Foundation Trust
- Halton Haven Hospice
- GP Health Connect
- Widnes Highfield Health

- Halton Borough Council

Name	
Role	
Organisation	
Signature	
Date	

Appendix 1: Privacy Impact Assessment

Description of Project	This project aims to develop a community wide data sharing agreement to underpin the sharing of patient records with the aim of supporting direct care delivery via the use of the EMIS Web clinical system. The shared record will be available to support the care management of patients within various services across Halton and therefore accessed by staff who have a legitimate relationship with the patient. The aim is that this will supersede previous multiple data sharing agreements and provide one over-arching agreement centred around the same principles and processes that all partners utilising an EMIS Web system will adhere too. This will include Halton Urgent Care Centres, adult community services, the extended access GP service and a number of Halton Interface services. The agreement will underpin the data sharing technical functionality within EMIS and provide the principles and basis for accessing the data. The data sharing functionality within EMIS provides a 'shared record view'. This provides only a view of the shared information and the information cannot be added to/or amended within a sharing partners host system. The availability of a shared record appears as a tab alongside the patients clinical record. If the reviewing clinician requires additional information that may be available within a shared record, for example, information that may be held within a GP record, the clinician will click the shared record tab. They can then search on a specific code or a view a recent investigation etc. as relevant and pertinent to the consultation.
Description of Data	The data to be accessed (via direct EMIS to EMIS data sharing) will include any information relevant to the consultation being undertaken. This will include demographic details, clinical history, medication etc. This information will be used to support the review being undertaken of the patient. The data being accessed will be part of a shared record. For example if a patient attends an MSK appointment, if deemed necessary by the clinician, the patients shared record can be

	viewed. The data being viewed will remain in the host system however a view of all available EMIS information will be available to the clinician to support their consultation. Information within the shared record will be displayed in chronological order. The clinician will then be able to search on specific codes within the shared record to identify information pertinent to the consultation. A number of exclusion codes will also be applied to the sharing agreement based on sensitive codes that are not appropriate for wider sharing.
What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?	The data is accessed in relation to a specific patient as part of the care management of that patient. For example, if a patient attends an extended access appointment with GP Extra, the assessing GP will access the record for that individual patient to inform and support the consultation being undertaken. As such the data needs to be identifiable as it is linked to the patient who has attended the service in relation to their direct care.
Will the information be new information as opposed to using existing information in different ways?	This information is currently collected and stored across the health economy as part of the clinical record keeping process. As such, this is not new information and will have been collated as part of previous consultations. This type of data is already being shared in this way by a number of services (in line with previous data sharing agreements). The intention of this project is to expand the range of this data sharing agreement to incorporate all EMIS sites within Halton and fully utilise the interoperability functionality that is available to support the delivery of care to Halton residents.
What is the legal basis for the processing of identifiable data?	The legal basis for the processing of identifiable data is direct care. All individuals accessing the shared record will have a legitimate relationship with the patient and will have been provided with the appropriate access within the clinical system relevant to their role to do so. User roles are assigned by system controllers within the organisations listed within the data sharing agreement which is managed as part of the user setup process.
If consent, when and how will this be obtained and recorded?	N/A
Who will be able to access identifiable data?	Access to the EMIS Web system is role based either via user login or the use of SMART cards. As such the level of access given to a user will be controlled by the system administrator within the respective organisation. Organisations will have their own governance policies to ensure that each user is

	provided with an individual and secure login to access the system based on their individual role by their system administrator. All users who will be accessing a shared record will be part of Halton primary care or a commissioned service and will therefore have a legitimate relationship with the patient as part of the their contractual arrangement with the CCG.
Will the data be linked with any other data collections?	The data sharing functionality available via EMIS to EMIS allows two instances of EMIS to be linked via the patient demographics. So this project will link the clinical records held within individual clinical systems to provide a shared record view.
How will this linkage be achieved?	This data is linked via the patient demographics. When a patient is registered within a clinical system they are traced from the NHS spine to ensure that records are matched via a central system and duplicates are not created.
Is there a legal basis for these linkages?	The legal basis for the linkage is direct care of the patient.
What security measures will be used to transfer the data?	No data is being transferred as part of this project. Data will remain in the host EMIS system which is hosted on a secure N3 connection. A read only view of data is provided by the shared record access but no data is transferred into the viewing system.
What confidentiality and security measures will be used to store the data?	The data is stored within the EMIS Web system via a secure N3 connection which is compliant with relevant data security standards. The data centre is based within the EEA. A shared view can only be accessed once a patient is registered with a service and therefore the service has a legitimate relationship with the patient as part of their commissioned service. Organisations will have their own security and governance policies to ensure that devices are locked when staff are away from desks and each user is provided with an individual and secure login to access the system along with access rights based on their individual role by their system administrator.
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	Within the EMIS Web clinical system, is the functionality to archive clinical records when a patient is either discharged or deceased but it is not possible to permanently delete a record from the clinical system. The archive functionality will be utilised to align to the NHS Records Management Code of Practice for retention periods.
What governance measures are	Access to EMIS systems is provided via role-based access and is

in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or anoth	managed via the system administrator within each organisation. In line with this PIA, data can only be accessed where the viewer has a legitimate relationship with the patient as part of direct care. Data is not transferred as part of this project and therefore cannot be disclosed to any third party organisations. Access to shared data will be reviewed on a regular basis by the system administrator and when functionality is available at an aggregated CCG level via the Business Intelligence Team.
If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA?	It is anticipated that should this be required, a separate record will be extracted from the relevant host EMIS system. For example if the request relates to an extended access appointment, the information will be extracted from the extended access EMIS system.
Is there functionality to respect objections/withdrawals of consent?	N/A as the legal basis for accessing the shared record is direct care so consent is not required in this instance.
Are there any plans to allow the information to be used elsewhere either in the CCG, wider NHS or by a third party?	There are no plans for the information specified in this PIA to be used for any other purpose than those specified.
Does any data flow in identifiable form? If so, from where, and to where?	Data does not flow between systems as part of this project. A view of shared data, available within EMIS systems is made available via the EMIS shared record functionality. This is configured on an organisational basis and is only available for services utilising EMIS Web systems. Data within the share record will always remain within the host systems.
Media used for data flow?	Data is accessed via the EMIS Web clinical system which is hosted on a secure N3 connection.

Appendix 2: Exclusion Codes

Code set	Clinical term
13N5.	HIV risk lifestyle
43C%	HTLV-3 antibody test
43WK.	Human immunodeficiency virus antibody level
43d5.	HIV antibody/antigen (Duo)
43h2.	HIV 1 PCR
43W7.	HIV1 antibody level
43W8.	HIV2 antibody level
4J34.	HIV viral load
62b..	Antenatal HIV screening
65P8.	AIDS contact
65QA.	AIDS carrier
65VE.	Notification of AIDS
67I2.	Advice about HIV prevention
6827.	AIDS (HTLV-III) screening
8CAE.	Patient advised about the risks of HIV
A788%	Acquired immune deficiency syndrome
A789%	Human immunodef virus resulting in other disease
AyuC4	[X] HIV disease resulting in other infectious and parasitic diseases
Eu024	[X] Dementia in human immunodef virus [HIV] disease
R109.	[D]Laboratory evidence of human immunodeficiency virus [HIV]
ZV018	[V] Human immunodeficiency virus – negative
ZV019	[V] Contact with and exposure to human immunodeficiency virus
ZV01A	[V] Asymptomatic human immunodeficiency virus infection status
ZV19B	[V] Family history of human immunodeficiency virus [HIV] disease
ZV6D4	[V] Human immunodeficiency virus counselling
ZV737	[V] Special screening examination for human immunodeficiency virus
1415.	H/O: venereal disease
14OP	At risk of sexually transmitted infection
43U%	Chlamydia antigen test
65P7.	Venereal disease contact
65Q9.	Venereal disease carrier NOS
6832.	Venereal disease screening
A780.	Molluscum cantagiosum
A7812	Genital warts
A78A.	Chlamydial infection
A78A3	Chlamydial infection of pelviperitoneum and other genitourinary organs
A78AW	Chlamydial infection, unspecified

A78AX	Chlamydial infection of genitourinary tract, unspecified
A9%	Syphilis and other venereal diseases
EGTON34	Chlamydia infection
L172%	Other maternal venereal diseases during pregnancy, childbirth and the puerperium
ZV016	[V] Contact with or exposure to venereal disease
ZV028	[V] Other venereal disease carrier
ZV745	[V] Screening for venereal disease
1543%	H/O: abortion
6776.	Preg. termination counselling
7E066	Hysterotomy and termination of pregnancy
7E070	Dilation of cervix uteri and curettage of products of conception from uterus
7E071	Curettage of products of conception from uterus NEC
7E084	Suction termination of pregnancy
7E085	Dilation of cervix and extraction termination of pregnancy
7E086	Termination of pregnancy NEC
8H7W.	Refer to TOP counselling
8M6..	Requests pregnancy termination
956%	HSA1-therap. abort. green form
9Ea%	Reason for termination of pregnancy
L05%	Legally induced abortion
L06%	Illegally induced abortion
ZV26%	[V] Infertility management {?all daughter codes}
8C8%	Treatment for infertility
7E0A%	Introduction of gamete into uterine cavity
7E1F2	Endoscopic intrafallopian transfer of gamete
9U%	Complaints about care
13H9.	Imprisonment record
13HN	Criminal Record
13HQ.	In prison
13I71	Husband in prison
14X4	On sex offenders register
2JC	Medically fit adjudicationyoung offenders
6992.	Prison medical examination
EMISNAC814	Accorn status: Young offenders institution
EMISNAC815	Accorn status: Bail/probation hostel
EMISNQSC1	Schedule 1 offender
EMISNQY03	Young Offender
EMISQAC759	Accorn location: Young offenders institution
T776.	Place of occurrence of accident or poisoning, prison
ZV4J4	[V] Conviction in civil and criminal proceedings without imprisonment
ZV4J5	[V] Problems related to release from prison

ZV625	[V] Imprisonment
14X..	History of abuse
1J3..	Suspected child abuse
SN55.	Child maltreatment syndrome
SN571	Sexual abuse
TL7..	Child battering and other maltreatment
TLx4.	Assault by criminal neglect
ZV19C	[V] Family history of physical abuse to sibling
ZV19D	[V] Family history of physical abuse to sibling by family member
ZV19E	[V] Family history of sexual abuse to sibling
ZV19F	[V] Family history of sexual abuse to sibling by family member
ZV19G	[V] Family history of mental abuse to sibling
ZV19H	[V] Family history of mental abuse to sibling by family member
ZV19J	[V] Family history of sibling abuse NOS
ZV19K	[V] Family history of sibling abuse by family member NOS
ZV4F9	[V] Problems related to alleged sexual of abuse child by person outside primary support group
ZV4G4	[V] Problems related to alleged sex abuse child by person within primary support group
ZV4G5	[V] Problems related to alleged physical abuse of child
ZV612	[V] Child abuse
TL01	Sexual Assault
ZV6D3	[V] Cousel related/combined conern regard sex attitude/behaviour
1K4	Gender reassignment
E225	Transexualism
EMISNQGE23	Gender reassignment
13I8	Adoption of child
6981	Adoption medical examination
8GE8	Adoption
9F5%	BAAF B1/2-adopt:birth history
9F6%	BAAF C/D-adopt:child report
EMISNQH120	Child legal status - freed for adoption
EMISNQH362	Child no longer for adoption
ZV703	[V]Adoption medical

Appendix 3: NHS Codes of Practice

Record Type	Retention start	Retention period	Action at end of retention period	Notes
GP Patient records	Death of patient	10 years after death - see Notes for exceptions	Review and if no longer needed destroy	If a new provider requests the records, these are transferred to the new provider to continue care. If no request to transfer: - Where the patient does not come back to the practice and the records are not transferred to a new provider the record must be retained for 100 years unless it is known that they have emigrated - Where a patient is known to have emigrated records may be reviewed and destroyed after 10 years - If the patient comes back within the 100 years, the retention reverts to 10 years after death.
Electronic Patient Records System (EPR) **NB: The IGA is undertaking further work to refine the rules for record retention and to specify requirements for EPR systems**	See Notes	See Notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.

GP Patient records	Death of patient	10 years after death - see Notes for exceptions	Review and if no longer needed destroy	If a new provider requests the records, these are transferred to the new provider to continue care. If no request to transfer: - Where the patient does not come back to the practice and the records are not transferred to a new provider the record must be retained for 100 years unless it is known that they have emigrated - Where a patient is known to have emigrated records may be reviewed and destroyed after 10 years - If the patient comes back within the 100 years, the retention reverts to 10 years after death.
Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.