Belfast Health and Social Care Trust

Use of Redaction – Guidance for Staff

Belfast Health and Social Care Trust

Contents Page

Introduction	2
What is Redaction	2
The Legislation	2
Legal Requirements	3
Prior to Redaction	3
Redaction process - Paper Records	4
Redaction process - Electronic Records	5
Other Considerations	5
Appendix 1	8
Contact Details	13

Introduction

Under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 an individual has a right of access to any personal data held about them. The following guidance has been drawn up to assist staff prepare records for release.

What is Redaction?

Redaction is the process which allows us to separate disclosable from non-disclosable information .By obscuring individual words, sentences, paragraphs or whole pages, documents can be released. The requestor can see that whilst there is information held, they have no legal right to access this data.

The Legislation

The main legislation which underpins the release of information is:

- **The UK General Data Protection Regulation 2018 (UK GDPR)**
- **Data Protection Act 2018 (DPA)**
- **Access to Health Records (NI) Order 1993 (AHR)**

Data Protection legislation allows individuals the right to access and receive a copy of their own personal information. This applies to all personally identifiable information held by the organisation.

Requests can be from the 'data subject' (the person the information is about); or by someone with authority to act on their behalf. Someone requesting access to another individual's personal information (e.g. a solicitor or family member) must have the appropriate authority to do so (usually written consent) and be seen to be acting on behalf of and in the best interests of that person. Enduring Power of Attorney will only allow access to relevant financial records not care and medical information unless otherwise stated.

A deceased patient/ client's **health** records can be requested under the Access to Health Records (AHR) Order by the legally appointed personal representative of the deceased or by anyone having a claim arising out the death. As the duty of confidentiality remains after death, careful consideration should be given to any request for access to a deceased patient's personal information. Family members do not have an automatic right of full access to their deceased relative's health records.

It should be noted that there is no equivalent legislation for deceased social care records.

When an individual's confidential healthcare or social care notes are released to a 3rd party, the information disclosed should be limited to what is necessary for the stated purpose. Please see the Trust's Access to Records Policy

Legal Requirements

The Trust is not obliged to supply any information unless it has received:

- A request (in writing or verbally) from the individual or his/her parent or guardian (where the child's consent has been obtained if they are over 13 years) or Solicitor, other advocate or organisation/body with a legal right of access.

- Proper assurances as to the identification of the individual requesting the records.

- Informed consent from the applicant about whom records have been sought.

- On receipt of all of the above, the Trust has a calendar month to respond and up to 90 days should the case be deemed as complex. The Trust has defined a complex case where the records requested :-
    - Cross over more than one Service area.
    - There are more than one volume / file of records.
    - Retrieval is required from hybrid systems i.e. manual and electronic systems.
    - Where other professionals are required to assess the risk to patient / client wellbeing in releasing the records.
    - Historical information has been requested.

Prior to Redaction

- Each service area should make sure that relevant professional staff are identified to review the records.

- The Trust provides redaction training on a regular basis contact DataProtection@belfasttrust.hscni.net for further information.

- Where possible staff should have a good knowledge of the records or nature of the records being reviewed for release and be able to identify information that may be exempt (see **Appendix 1 –** More commonly used Legal Exemptions from the Data Protection Act 2018).

- You should always check the requirements on the request/Solicitor's letter/SPNI Form 81 to see exactly what is needed. Records may only be required for a particular time period or for a particular incident. The requestor may not be clear what's available in the record so will ask for everything. It might be worth having a discussion with the requestor as this could minimise the work required.

- Professional staff may want to check the consent provided, often patients/clients are not aware of the extent of records being sought even though they have signed it off. Consent should be informed.

- All requests from other Agencies for personal data e.g. from Banks, Building Societies and Solicitors should have the data subject's written authorisation for disclosure of their records for that specific purpose.

- If it is a request from another organisation, the Trust via the Data Protection Office may need to check the legal basis for providing data if consent has not been provided.

- The PSNI use a Form 81 to request information. This is a voluntary sharing of records but best practice would always dictate that there is consent from the data subject to process their information. If a professional is concerned about releasing the information, the Trust can request that the Police obtain a Court Order. However where the information is required for the detection, prevention of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty or an imposition of a similar nature; the Trust can legally provide the information without consent, redaction therefore may be less restrictive to provide the necessary information (see **Appendix 1** – Data Protection Act 2018 Part 1 -*ADAPTATIONS AND RESTRICTIONS BASED ON ARTICLES 6(3) AND 23(1) Crime and taxation: general)*

- Records requested under a Court Order **DO NOT** have to be redacted. If a professional does not believe that the records are related to the court case in question, a letter can be written to the Judge to explain the rationale. Do not send the original records to Court unless specifically told to do so (see **Appendix 1** – Data Protection Act 2018 – *Information required to be disclosed by Law etc or in connection with Legal Proceedings*).

Redaction Process – Paper Records

There are a range of redaction methods for hard copy records. The end result must ensure that the redacted material cannot be seen or guessed due to incomplete redaction.

Redaction should always be carried out on **single page copies** of the paper record.

Blacking out – the most common method is to photocopy the original document and use a black marker pen on the photocopy to block out the sensitive material.

This means checking to make certain that words cannot be made out when the document is held up to light or that the ends, top or bottom of text are not visible.

The redacted version should then be photocopied again to produce a releasable version. This further photocopy is necessary as information redacted using marker pen can still be read when held up to light. Always check this even after photocopying a second time.

The Trust uses software - **Objective Redact**, which can assist in redacting if the original records are scanned into a PDF format. Advice can be sought from the Data Protection Office on this product and its use.

Redaction Process - Electronic Records

The redaction of born-digital records is an area of records management practice which raises unique issues and potential risks due to the inclusion of metadata underneath the visible record.

Never redact the original or master version of an electronic record - redaction must always be carried out on a new copy of the record (e.g. 'save as' a working version to carry out the redaction). Delete all restricted information, either by using the black highlighter tool; or by replacing it with the text string [redacted]. This will ensure that redaction is apparent but the space cannot be used to identify the missing information.

It is essential that any redaction technique is secure to eliminate the possibility of redacted information being recovered. Redaction must irreversibly remove the required information from the redacted copy of the record. The information must be completely removed from the meta data, not simply from the displayable record.

For electronic records, which can be printed as a hardcopy, traditional redaction techniques as described in this document can be applied to the printed hard copy.

For additional security and to reduce risk of software being used to recover the redacted information from the PDF version, you should print and rescan the document before sending electronically.

Other Considerations

- The focus of the information needs to be on the applicant whose information is requested.
- All personal health and social care records should be reviewed, redactions quality assured and authorised for release by the person in charge of patient/client care and treatment (e.g. Consultant(where required), Team Manager, Key-worker and/or other professional staff currently involved with the patient/client).
- Other staff that had previous involvement in the case may need to be consulted for their views on release.
- Where a staff member has left the Trust it is the responsibility of those with current responsibility of that service area to approve release of the notes and records.
- For Multi-Disciplinary records each staff group / profession should review the relevant section of records.
- If you are providing acute hospital notes and records then please check with the Medical Legal Department about the authorisation for release and review as not all acute notes require professional sign off.

- Notes and records should also be checked by each service area for accuracy in terms of correct filing. Any misfiled information (e.g. relating to a different patient) should be removed by the service and brought to the immediate attention of the Ward / Team Manager.

- Redaction is carried out in order to exempt details from a document. It should be used to remove third party data e.g. names of other patients, contact details, sensitive information, names and details of other family members etc. This can in some instances include pronouns or plurals where, to include them, would identify individuals through context. Be sure also to remove personal contact details or sensitive information (**Appendix 1** – *Schedule 3 Part 2 Health Data and Schedule 3 Part 3 Social Work Data*).

- To comply fully with requests for information, staff must redact exempt material only. A whole sentence or paragraph should not be removed if only one or two words are non-disclosable, unless release would place the missing words in context and make their content or meaning clear.

- Take great care to ensure that the non-disclosable material cannot be deciphered from the location pattern, length (e.g. of a name), the associated un-redacted text (i.e. within the context of other information released). This may mean disguising the size and shape of the redacted (blacked out) content.

- Reviewers should also check records for other copies or entries of the same information or documents so that they carry out redaction consistently throughout (i.e. do not redact exempt information in one part of a file but disclose it in another section).

- Once redactions have been identified and agreed, the decisions for withholding data should be recorded. This might require keeping a copy of the records released for up to three years, with a note explaining the reasons for redaction.

- If any information has been redacted, please be clear what legal exemptions apply (see **Appendix 1**).

- No changes or amendments should be made to records held unless it would have happened regardless of the receipt of the request being made.

- A copy of the redacted documents released to the requestor should be held for a period of three years by the Service Area. This would allow for queries on why information has been redacted to be addressed

- If so much information has to be redacted that a document becomes nonsensical, the entire document should be withheld.

- Trust staff names for the Service where records have been requested are not redacted unless there is a significant reason - seek advice from the Data Protection Office.

- Names of staff from other Organisations or Services are not provided, but job titles can be provided.

- Personal data in relation to management forecasts, negotiations and references are not provided. See **Appendix 1**

- If there are drafts of letters, they should be included unless they are the subject of legal advice. This should include the most recent one especially if part of an email chain.

- Ensure photocopied records are in the correct order and reflect the content / layout of the original file

- The appropriate Line Manager should quality assure and sign off the Release of Records form where required (some acute records do not require authorisation to release)

All subject access requests, Court Orders and Form 81's are processed via two main locations within the Trust :-

1. Community sites, including Knockbracken, Muckamore, staff and miscellaneous records - Data Protection Office
   Email: DataProtection@belfasttrust.hscni.net tel 02895 046955

2. Acute sites -
   Email: MedLegalServs@belfasttrust.hscni.net tel 028 95 040726

Appendix 1 More Commonly Used Legal Exemptions from the Data Protection Act 2018

There are limited exemptions to the right of access to personal information. Access can be denied or restricted for the following reasons:

- Legal advice is not provided as it is legally privileged. – Please see **below**

- Third Party Information: - the information relates to, or was provided by an individual other than the patient who could be identified from that information and who has not given consent for disclosure (see *Data Protection Act 2018 Part 3 – Restriction based on Article 23(1): Protection of Rights of Others).*

- Detriment: - in the view of the appropriate HSC professional, disclosure of the restricted information would cause serious harm to the physical and/or mental health of the patient / client or other individual(s) (See *Data Protection Act 2018 Schedule 3 Part 2 –UK Health Data and Part 3 UK Social Work Data*).

- The patient / client has expressly requested that some or all of the information should not be disclosed (e.g. in general or to named persons) (see *Data Protection Act 2018 Part 3 – Restriction based on Article 23 (1): Protection of Rights of Others (3e*) .

- Based on professional opinion and knowledge of the case: the 3rd party applicant is not acting in the patient's/client's best interests or is not authorised to access the requested information.

- Under AHR (deceased person's records) - access may only be given to those with the appropriate documentation showing legal authority to access the records. Where authority is in place, access will also be limited to information which is relevant to any claim.

Third Party Data

A decision on whether to release or redact information, particularly third party data, should be taken on a case-per-case basis and based on the individual circumstances and knowledge of the case and associated records; however the following points are a guide to the type of issues to consider:

- Is there information relating to / about someone else?
- Is there consent from the third party to disclose?

In the absence of consent of the other individual:

- Is it reasonable to disclose in the circumstances?
- Is there a duty of confidentiality owed to the third party?
- Has consent been refused and valid reasons given?
- Can you redact the third party information?

Also consider what is already known to the applicant?

- Legislative considerations – Children (Northern Ireland) Order 1995
- Anonymity of complainants
- What is the risk of 'jigsaw attack' i.e. piecing together bits of information to create a more complete picture of someone?
- Has the information been provided in confidence by a third party?
- Does the information constitute legal advice or correspondence (not to be disclosed)?
- Is the information likely to cause serious harm to the physical or mental health of any person, if disclosed?
- The names of senior staff or staff involved in a person's healthcare or social care are unlikely to be redacted.
- Court Papers, position Papers, Summons or Court Reports do not have to be provided. This would also be true for reports from the Guardian ad Litem Service.

Data Protection Act 2018 PART 1

ADAPTATIONS AND RESTRICTIONS BASED ON ARTICLES 6(3) AND 23(1)
Crime and taxation: general
2(1) The listed UK GDPR provisions and Article 34(1) and (4) of the UK GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes—
(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

Data Protection Act 2018 PART 1

Information required to be disclosed by law etc or in connection with legal proceedings
5(1) The listed UK GDPR provisions do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public, to the extent that the application of those provisions would prevent the controller from complying with that obligation.
(2) The listed UK GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.

(3) The listed UK GDPR provisions do not apply to personal data where disclosure of the data—

(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights, to the extent that the application of those provisions would prevent the controller from making the disclosure.

PART 3 Restriction based on Article 23(1): Protection of Rights of Others

Protection of the rights of others: general

16(1)Article 15(1) to (3) of the UK GDPR (confirmation of processing, access to data and safeguards for third country transfers), and Article 5 of the UK GDPR so far as its provisions correspond to the rights and obligations provided for in Article 15(1) to (3), do not oblige a controller to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information.

(2) Sub-paragraph (1) does not remove the controller's obligation where—

(a) the other individual has consented to the disclosure of the information to the data subject, or

(b) it is reasonable to disclose the information to the data subject without the consent of the other individual.

(3) In determining whether it is reasonable to disclose the information without consent, the controller must have regard to all the relevant circumstances, including—

(a) the type of information that would be disclosed,

(b) any duty of confidentiality owed to the other individual,

(c) any steps taken by the controller with a view to seeking the consent of the other individual,

(d) whether the other individual is capable of giving consent, and

(e) any express refusal of consent by the other individual.

(4) For the purposes of this paragraph—

(a) “information relating to another individual” includes information identifying the other individual as the source of information;

(b) an individual can be identified from information to be provided to a data subject by a controller if the individual can be identified from—

(i) that information, or

(ii) that information and any other information that the controller reasonably believes the data subject is likely to possess or obtain.

Assumption of reasonableness for health workers, social workers and education workers

17(1) For the purposes of paragraph 16(2)(b), it is to be considered reasonable for a controller to disclose information to a data subject without the consent of the other individual where—

(a) the health data test is met,

(b) the social work data test is met, or

(c) the education data test is met.

(2) The health data test is met if—

(a) the information in question is contained in a health record, and

(b)the other individual is a health professional who has compiled or contributed to the health record or who, in his or her capacity as a health professional, has been involved in the diagnosis, care or treatment of the data subject.

(3) The social work data test is met if—

(a) the other individual is—

(i) a children's court officer,

(ii) a person who is or has been employed by a person or body referred to in paragraph 8 of Schedule 3 in connection with functions exercised in relation to the information, or

(iii) a person who has provided for reward a service that is similar to a service provided in the exercise of any relevant social services functions, and

(b) the information relates to the other individual in an official capacity or the other individual supplied the information—

(i) in an official capacity, or

(ii) in a case within paragraph (a)(iii), in connection with providing the service mentioned in paragraph (a)(iii).

(4) The education data test is met if—

(a) the other individual is an education-related worker, or

(b) the other individual is employed by an education authority (within the meaning of the Education (Scotland) Act 1980) in pursuance of its functions relating to education and—

(i) the information relates to the other individual in his or her capacity as such an employee, or

(ii) the other individual supplied the information in his or her capacity as such an employee.

(5) In this paragraph—

“children's court officer” means a person referred to in paragraph 8(1)(q), (r), (s), (t) or (u) of Schedule 3;

“education-related worker” means a person referred to in paragraph 14(4)(a) or (b) or 16(4)(a), (b) or (c) of Schedule 3 (educational records);

“relevant social services functions” means functions specified in paragraph 8(1)(a), (b), (c) or (d) of Schedule 3.

Legal Professional Privilege

19The listed UK GDPR provisions do not apply to personal data that consists of—

(a) information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings, or

(b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

Management forecasts

The listed UK GDPR provisions do not apply to personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned.

Negotiations

The listed UK GDPR provisions do not apply to personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice those negotiations.

Confidential references

24. The listed UK GDPR provisions do not apply to personal data consisting of a reference given (or to be given) in confidence for the purposes of—

(a)the education, training or employment (or prospective education, training or employment) of the data subject,

(b)the placement (or prospective placement) of the data subject as a volunteer,

(c)the appointment (or prospective appointment) of the data subject to any office, or

(d)the provision (or prospective provision) by the data subject of any service.

Schedule 3 PART 2 U.K. Health data

(2) For the purposes of this Part of this Schedule, the "serious harm test" is met with respect to data concerning health if the application of Article 15 of the UK GDPR to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

Schedule 3 PART 3 U.K. Social work data

(2) For the purposes of this Part of this Schedule, the "serious harm test" is met with respect to social work data if the application of Article 15 of the UK GDPR to the data would be likely to prejudice carrying out social work, because it would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

This guidance draws upon ***"****The National Archives Redaction toolkit - Editing exempt information from paper and electronic documents prior to release".* This 'Redaction Toolkit' is

aimed at all authorities subject to the Freedom of Information Act (FOIA), Data Protection
legislation (UK GDPR and DPA 2018) and the Environmental Information Regulations (EIRs).

For more detailed advice and guidance see:

http://www.nationalarchives.gov.uk/documents/information-management/redaction_toolkit.pdf

Or contact:
The Data Protection Office
Main Administration Building
Knockbracken Health Care Park
Saintfield Road
Belfast
BT8 8BH
Email: DataProtection@belfasttrust.hscni.net Tel: 02895 046955