Insert here the logo
of the
signatory organisation

External Ref:	HIG 01
Review date	November 2016
Version No.	V07
Internal Ref:	ERYC CFS ILS 02

Humber Information Sharing Charter

This Charter may be an uncontrolled copy, please check the source of this document before use.

The latest version of the Charter can be found on the Humber data observatory website along with a list of the Charter signatories

http://www.humberdataobservatory.org.uk/legal

This Charter supersedes all previous versions of this Charter including the Community Charter for Information Sharing (North East and North Lincolnshire) and the General Protocol for Information Sharing between agencies in Kingston upon Hull and the East Riding of Yorkshire.

Contents

Humber Information Sharing Charter

1. Introduction
2. Objectives of the Charter
3. Our Commitment
4. Designated Officer
5. The principles guiding the sharing of information
6. Tier 2 Information Sharing Agreements
7. Information Security
8. Signatory organisations to this Charter
9. Complaints
10. Freedom of Information
11. Monitoring and Review
12. Humber Information Governance Group
13. Partnership Undertaking

Humber Information Sharing Charter

1. Introduction

1.1 The appropriate exchange of information is essential to deliver effective and efficient services for our citizens, to meet their needs and ensure their welfare and protection. However there is a balance between the need to share sufficient information to deliver effective services, and preserving the privacy of the individual.

1.2 To assist understanding and the application of effective information sharing it is helpful to have locally documented clarity about how legal constraints 'fit' with practice guidelines, identifying what can and cannot be shared with whom, how and for what purposes.

1.3 This Charter provides a two-tier framework for the effective and secure sharing of information in accordance with legal requirements, ethical boundaries and good practice across the Humber region. It will ensure transparency of information governance practices, assist the documenting of information sharing decisions and actions to ensure they are auditable, and raise awareness of the legal and ethical boundaries around information disclosure and the rules and methods for accessing data.

1.4 Tier 1 (The Charter) establishes the Principles and standards under which information sharing will take place.

1.5 Tier 2 (The Agreements) identifies the operational requirements in place for the sharing of information for a specific and lawful purpose.

1.6 Whilst there will only be one Tier 1 Charter, there will be many Information Sharing Agreements.

1.7 The Charter does not impose new obligations on signatory organisations, but reflects current regulations and legislation for the sharing of personal information, and builds on existing partnerships.

2. Objectives of the Charter

2.1 The signatories to this Charter recognise the importance of sharing information effectively and securely for the purposes of delivering and improving outcomes for the citizens and communities we serve across the Humber Region.

2.2 Through this Charter the signatories aim to achieve consistent and good practice for the sharing of personal information.

- Providing signatory organisations and those acting on their behalf with clear guidelines to follow for the secure and confidential sharing of personal information in accordance with legal requirements.

- Informing citizens why personal information about them may need to be shared between signatory organisations, and how that information will be shared and used.

3 Our commitment

3.1 As a signatory organisation we are committed to ensuring that the identifiable personal information we collect, hold and use will be processed in accordance with legislation, best practice and the expectations of citizens, to meet and ensure security and confidentiality requirements. This Charter sets out the principles and minimum standards that will underpin the processing and exchange of personal information.

4 Designated Officer

4.1 As a signatory organisation we must have in place a Designated Officer, responsible for approving and monitoring the processing of personal information in accordance with the Humber Information Sharing Charter.

4.2 For Health and Social Care organisations this will be the Caldicott Guardian or the Senior Information Risk Owner, for organisations signed up to Public Service Networks it will be the Senior Information Risk Officer. For all other organisations it will be a senior officer with responsibility for information governance nominated by the Chief Executive or equivalent.

5 The principles guiding the sharing of information

5.1 As a signatory organisation we will work to:

a) Support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymous information in accordance with our legal, statutory and common law duties, and the requirements of this Charter and other additional guidance as notified to us;

b) Ensure a copy of the Charter and the identity of the Designated Officer are clearly and widely promoted across the organisation and available to all;

c) Have in place effective policies and procedures to meet our responsibilities for the secure and confidential sharing of information, aligned to statutory requirements and this Charter;

d) Ensure that all employees and those acting on our behalf are aware of, understand and comply with their responsibilities for information security and confidentiality through appropriate promotion, training, monitoring and enforcement;

e) Ensure all our data meets the high standards identified in the Audit Commission's "Improving information to support decision making: standards for better quality data", November 2007, and any locally agreed protocols.

5.2 When sharing information we will endeavour to ensure that:

f) Individuals are fully informed about the information held about them and how it will be used and shared;

g) Information will be shared with consent, except where statutory requirements or common law principles support the disclosure or withholding of information;

h) Information is only shared when and where it is necessary and justified for a lawful and specified purpose;

i) Only the minimum identifiable information that is required for the purpose is shared. The information shared should be relevant, proportionate and not excessive for specified purpose, and be defined by the appropriate Tier 2 Protocol.

j) Wherever possible statistical or aggregated and anonymous information is provided, to eliminate the risk of individuals being identified;

k) Only information actually needed for the purpose will be collected or shared;

l) Information is clearly identified as being fact, opinion, or a combination of the two;

m) Information is only used for the purposes for which it was collected or shared;

n) Information is kept and shared safely and securely, with appropriate safeguards in place to ensure only individuals with a legitimate right have access to it, preventing accidental or deliberate unauthorised access;

o) Information no longer needed for legal or administration requirements is disposed of in a safe and appropriate manner;

p) The capacity of a data subject, including children and vulnerable adults, to exercise their right to provide or refuse consent will be considered on an individual case by case basis; and

q) Considerations of confidentiality and privacy will not automatically cease on death.

6 Tier 2 - Information Sharing Agreements

6.1 The focus of each agreement is the particular **purpose** underlying the need to share, who is sharing the information, the specific information being shared, the legal basis for the sharing of the information and the processes in place to ensure that the information is securely exchanged and managed.

6.2 Each Protocol describes the common contexts and shared objectives between signatory organisations delivering services of a similar scope, defines the type of information to be shared, the purposes for which it can be shared, and the underpinning legislation and the associated duties and powers that enable legally justifiable exchanges of information for that purpose based on the principles and standards set out in the Charter.

6.3 Tier 2 Agreements will be signed on behalf of each partner by a senior manager, with responsibility for operational delivery.

7 Information Security

7.1 It is assumed that each signatory has achieved or will aim to work towards information security standards such as ISO 27001, or a similar level of compatible security.

7.2 Each signatory is encouraged to have an Information Security Policy in place setting out the minimum standards of security they require. Where a specific policy is not in place the following principles must be followed at all times to ensure personal data is appropriately protected to prevent unauthorised access, disclosure, deletion or alteration:

a) Unauthorised officers and other individuals are prevented from gaining access to personal data;
b) Visitors must be supervised at all times;
c) All electronic systems containing personal data must be password-protected, to prevent unauthorised access;
d) Passwords must be treated as private to the individual and NOT disclosed to others;
e) All electronic devices including PCs, laptops and smartphones must be 'locked' when unattended or not in use;
f) All personal data stored on mobile electronic devices such as laptops, USBs, smartphones etc, must be protected by encryption;
g) All resources (including mobile devices, printouts) containing personal data must be placed in secure locations when not in use, and only accessible to authorised officers;
h) Anti-virus checks are undertaken on software / removable media prior to use on networks / machine;
i) All documents exchanged are protectively marked according to their sensitivity using the Government Protective Marking Classification Scheme;
j) Caution is exercised in the use of e-mail, recipients are checked and personal data is only exchanged using secure e-mail;
k) Caution is exercised in the use of fax communications, the intended recipient of a fax containing personal data must be aware that it is being sent and has ensured security on delivery;
l) Where personal data is removed from a secure environment, appropriate security measures must be in place to keep it secure and protected;
m) Caution is exercised in the use and transport of personal data outside of its secure environment or in the public domain to prevent loss or unauthorised disclosure;
n) Information must be disposed of securely; and
o) Personal data must not be disclosed to anyone other than the data subject unless you have their consent, or it is a registered disclosure, required by law, or permitted by a Data Protection Act 1998 exemption.

8 Signatory organisations to this Charter

8.1 A list of the organisations that have signed up to this Charter, and have agreed to adopt the principles and standards set out in it and the supporting agreements is available on the Humber data observatory website (http://www.humberdataobservatory.org.uk/legal)

9 Complaints

9.1 A complaint from a data subject or their representative about information held under the terms of this Charter will be investigated first by the signatory organisation receiving the complaint.

9.2 Where a complaint identifies that any part of the Charter needs to be reviewed, this action must be taken by the Humber Information Governance Group.

10 Freedom of Information

10.1 The Freedom of Information Act and Environmental Information Regulations gives a general right of access to the information public authorities hold. Any requests for information in relation to the Charter must be passed to the signatory organisation's Freedom of Information Officer to deal with.

10.2 Requests for Tier 2 Agreements will need to consider if the disclosure of any elements would compromise the procedures in place for the security and protection of the personal information, and potentially be subject to an exemption to disclosure.

11 Monitoring and Review

11.1 As a signatory to the Charter we agree to support the Humber Information Governance Group with the monitoring and 2 yearly review of the Charter and associated Tier 2 Agreements.

12 Humber Information Governance Group

12.1 The Humber Information Governance Group is a virtual Group representing public sector organisations and their partners across the Humber region.

13 Partnership undertaking

13.1 As a signatory to the Charter we accept the principles laid down in this document will provide a secure local framework between the signatory organisations for the secure sharing of personal information in a manner compliant with statutory and professional responsibilities.

13.2 On behalf of the organisation I represent, I confirm that we will undertake to comply with all relevant legislation and requirements relating to confidentiality, safe information sharing and disclosure, appropriate storage and destruction of information.

a) Implement and adhere to the standards and principles set out in this Charter whenever exchanging personal information, both with a co-signatories and other organisations;
b) Ensure that all Protocols and Procedures established for the sharing and confidentiality of information are consistent with this Charter;
c) Co-operate, as far is compatible with existing statutory responsibilities, with other signatories to ensure effective information sharing and reduce duplication.

13.3 Signatory

Organisation:	
Name:	
Position:	
Signature:	
Date:	