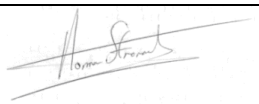
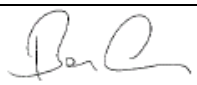
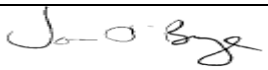
Information Sharing

Statement

CONTENTS

SIGNATORY PARTNER ORGANISATIONS

Organisation	Signature Position	Date
Borough Council of Wellingborough	 **Chief Executive**	13.08.13
Corby Borough Council	 **Chief Executive**	24.07.13
Daventry District Council	 **Chief Executive**	22.08.13
East Northamptonshire Council	 **Chief Executive**	05.08.13
Kettering Borough Council	 **Asst Chief Executive**	
Northampton Borough Council	 **Chief Executive**	24.07.13
South Northamptonshire Council	 **Chief Executive**	25.07.13
Northamptonshire County Council	 **Chief Executive**	24.07.13
Northamptonshire Police & Crime Commission	 **Chief Executive**	02.08.13
Northamptonshire Police	 **Chief Constable**	24.07.13
Nene Clinical Commissioning Group	 **Accountable Officer**	31.07.13
Corby Clinical Commissioning Group		
Northampton General Hospital		
Kettering General Hospital		
Northamptonshire Healthcare Foundation Trust		
Northamptonshire Youth Offending Service	 **Head of NYOS**	24.07.13
Northamptonshire Probation Service	 **Chief Executive**	07.08.13

1. Introduction

Information sharing is key to delivering improved, more efficient public services that are co-ordinated and meet the needs of individuals and their communities. However, legally, the privacy rights of the individual must be maintained whilst sharing information.

This statement, supported by the Information Commissioner's code of practice for sharing personal information and other guidance, sets out the commitment required from each partner organisation to share information legally with other partner organisations.

2. Purpose

The purpose of this statement is to promote the principles of information sharing in order to help deliver quality services, in a timely, efficient and secure manner whilst ensuring there is a specific and lawful purpose or consent obtained to allow the sharing of information to take place.

This statement is not, in itself, a licence to share information, but a mechanism to give assurance that there is common understanding and commitment to share information and a consistent approach between relevant organisations in relation to information protection and processing. The Northamptonshire Access to Information Group will monitor and review the shared approach and develop other tools and templates to support the principles of this statement as appropriate.

3. General Principles

This Statement recognises and promotes recommended good practice and legal requirements to be followed by all signatory organisations. It does not alter existing arrangements already in place for urgent sharing e.g. related to child protection.

Partner organisations intending to share information, whether ongoing or as part of a time-limited exercise such as a project, should complete an Information Sharing Agreement.

Systematic Information Sharing

Systematic information sharing involves routine sharing of data sets between organisations for an agreed purpose. Partner organisations who intend to share information systematically should complete an Information Sharing Agreement unless other regulations or legislation mean that an agreement is not required.

Ad-hoc Information Sharing

'One off' or 'ad hoc' information sharing involves any exceptional sharing activities for a range of purposes which are not covered by routine data sharing arrangements. For ad hoc activities, an Information Sharing Agreement is not needed. Advice should be sought from each organisation's Information Sharing contact where there is any doubt.

It is also good practice to record any ad hoc or one off data sharing activities detailing the circumstances, what information was shared and explaining why the disclosure took place. Remember, only share the minimum amount of data necessary and remove any fields or datasets which are not directly relevant before you share.

4. Scope

Signatories to this statement are from a number of different sectors, including health, local government, and police. Each signatory may have independent information processing standards and good practice guidance. By becoming a signatory to this statement each partner organisation is making a commitment to:-

a) Adopt and promote good practice standards for the processing of personal information in accordance with the relevant legislations.

b) Apply all good practice guidance relating to information sharing and handling, including the Information Commissioner's Data Sharing Code of Practice, Fair Processing and Best Practice Standards, the Ministry of Justice Guidance on the Law in Public Sector Data Sharing.

c) Adhere to the appropriate legal requirements for information sharing and information handling.

d) Be proactive in developing and reviewing Information Sharing Agreements where it is agreed to share information between partner organisations

e) Have procedures for upholding individuals' rights, particularly the right to subject access.

f) Provide effective information protection and confidentiality training to staff who process personal information

g) Have procedures for information security ensuring that safeguards are in place to prevent unauthorised or unlawful access.

h) Have procedures for the retention and disposal of personal information compliant with legal obligations and sector specific regulations.

i) Have internal procedures for managing serious information incidents, including possible privacy or security breaches and alerting the relevant information sharing partners when this occurs

5. The Legal Framework

Partner organisations will share information in accordance with and having due regard to the relevant law, the Caldicott Principles and the statutory Information Sharing Code of Practice issued by the Information Commissioner[1] and other relevant statutory and/or non-statutory guidance concerning the sharing and handling of information.

Individual Information Sharing Agreements will state the legislation, regulations and good practice guidance relevant to the specific need to share information between partner organisations.

6. Individual Responsibilities

Every individual working for the organisations that are signatory to this statement is personally responsible for the management of any information they obtain, handle, use and disclose and must be trained to carry out these duties.

---

[1] Information Sharing Code of Practice
http://www.ico.gov.uk/for_organisations/information_protection/topic_guides/information_sharing.aspx

Individuals should be made aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal, and potentially, criminal proceedings. Signatories should ensure that their organisations support this process through effective induction/refresher training (such as “protecting our data training” or information security training) where necessary.

7. Review

This Statement will be reviewed at least annually or as legislation and guidance requires.

If it is considered necessary to change this statement as a result of compliance, performance, legislative/regulatory change or for any other reason then a recommendation will be made from one or more of the signatory organisations to the other signatories for consideration. Changes will be agreed by the Chief Executives Group.

The first scheduled review will be in July 2014.

8. Termination

There is no requirement to terminate this agreement universally. Organisations wishing to withdraw must notify the other signatories.

9. Freedom of Information

This document is considered ‘unrestricted’ and may be published or provided in response to an FOI request by any of the signatory organisations.

RELEVANT LEGISLATION

Your ability to share information is subject to a number of legal constraints and other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence. If you wish to share information, you must consider whether you have the legal power or ability to do so. This is likely to depend on the nature of the information in question and on whom you are, and therefore what legislation applies to you.

Most public sector organisations derive their powers from statute. Before starting data sharing activities you should identify the relevant legislation for your organisation which defines the organisation's functions and the powers you may exercise in order to achieve your organisation's objectives. Broadly speaking, there are three ways an organisation may share data:

- **Express obligations** – where a public body is legally obliged to share particular information with a named organisation.
- **Express powers** – often designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways".
- **Implied powers** – often legislation regulating public bodies is silent on data sharing. In these circumstances, it may be possible to rely upon implied powers to share information derived from express provisions in legislation.

Express powers may allow organisations to do other things that are reasonably incidental to those which are expressly permitted.

Whatever the source of an organisation's power to share information, you must check that the power covers the disclosure in question – otherwise you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. For further information, consult your information sharing lead, data protection officer or legal services department. Also check whether there is sector-specific guides addressing the information sharing you intend to undertake, such as the DWP's Guidance for Local Authorities on the use of social security data (2010).

The following list – which is not exhaustive – highlights legislation with particular relevance to guiding data sharing decisions:-

I) Data Protection Act (1998) (DPA)

The Data Protection Act 1998 (DPA) governs the standards for processing personal data, including the collection, use of and disclosure of information. The legislation requires that data controllers meet certain obligations and it gives individuals certain rights with regard to their own personal data. The main standard for processing personal data is compliance with the 8 DPA principles listed below:-

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

a. at least one of the conditions in Schedule 2 is met, and

b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

II) Human Rights Act (1998) (HRA) Article 8

The Human Rights Act enacts the European Convention on Human Rights in the UK. Article 8 of the Convention gives everyone the right to respect for his private and family life, home and correspondence, and is especially relevant when sharing personal data. Article 8 is not an absolute right - public authorities are permitted to interfere with it when it is lawful and proportionate to do so.

It is advisable to seek specialist advice if the disclosure or data sharing arrangement you are proposing is likely to have an impact on privacy which engages Article 8 or any HRA rights. If you disclose or share personal data only in ways that are compliant with the DPA, the disclosure of that information is likely to comply with the HRA. Personal data is normally exempt under the HRA.

III) The Children Act (1989)

Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm. Section 47 states that the authorities listed below must assist a local authority with enquiries of this nature by providing relevant information, unless doing so would cause more harm or be considered unreasonable:

- any local authority;
- any local education authority;

- any housing authority;
- any health authority; and/or
- any person authorised by the Secretary of State.

IV) The Children Act (2004)

Section 10 of the Act places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area in relation to:

- physical and mental health, and emotional well-being;
- protection from harm and neglect;
- education, training and recreation;
- making a positive contribution to society; and/or
- social and economic well-being.

V) Civil Contingencies Act (2004) (CCA)

In emergencies, it may be in the interests of affected vulnerable people for their personal data to be shared with emergency responders as defined in the CCA 2004. Sharing personal information may help emergency responders to perform statutory duties. The CCA 2004 1(1) defines an emergency as “an event or situation which threatens serious damage to human welfare and/or the environment or war or terrorism which threatens damage to security”. The principles and legislative provisions related to information sharing apply to the planning, response and recovery phases of emergencies.

VI) The Common Law Duty of Confidence

The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are three categories of exception:

- Where there is a legal compulsion to disclose.
- Where there is an overriding duty to the public.
- Where the individual to whom the information relates consented.

Partners should consider which of these conditions are the most relevant for the purposes of an agreement. The guidance from the Information Commissioner states that because decisions to disclose ‘in the public interest’ involve the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking the decisions.

VII) Police Act (1996) (PA)

Section 30(1) of the PA gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines these powers as powers under any enactment whenever passed or made. These powers include investigating and detecting crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order.

Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff.

VIII) Crime and Disorder Act (1998) (CDA)

Section 115 of the CDA confers a power on any ‘relevant authority’ to exchange information which is ‘necessary’ or ‘expedient’ to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder.

Section 17 CDA requires that all Local Authorities (LAs) consider crime and disorder reduction while exercising their duties. Sections 5 and 6 of the CDA impose a general duty upon local authorities to formulate and implement a strategy for the reduction of crime and disorder in its area.

IX) Local Government Act (2000) (LGA)

The main power specific to Local Authorities (LAs) is section 2 LGA (2000) – the power of "well-being". This enables LAs to do anything to promote social, economic, or social well-being in their area provided the act is not specifically forbidden by other statute.

In addition, S111 LGA (1972) enables LAs to do anything conducive or incidental to the discharge of any of its functions, providing it has specific statutory authority to carry out those main functions in the first place.

The above are general powers for LAs but LAs have statutory powers relating to specific activities and these should be referred to as appropriate in any Information Sharing Agreements.

X) The Gender Recognition Act 2004 (GRA)

Under the Gender Recognition Act 2004 (GRA), individuals who have obtained gender recognition certificates (GRCs) in order to acquire legal status of their transitioned gender are entitled to legal protection from disclosure about their status. It is a criminal offence to disclose this status; i.e. if someone has a gender recognition certificate stating they are a woman, it is a criminal offence to disclose that they used to be a man, except where explicit consent has been obtained from the individual involved or the disclosure is for the purposes of proceedings before a court or tribunal.

GOVERNMENT SECURE DOMAINS

Domains that are secure **when used end to end** for the exchange of data are:

x.gsi.gov.uk

.police.uk

.cjsm.net

gsi.gov.uk

.pnn.police.uk

.scn.gov.uk

gsx.gov.uk

.mod.uk

.nhs.net

gse.gov.uk

x.gcsx.gov.uk