Document filename: HSCIC Privacy Impact Assessment 2013			
Directorate / Programme	Information Governance	**Project**	
Document Reference			
Project Manager	Clare Sanderson	**Status**	Final
Owner	Clare Sanderson	**Version**	2.0
Author	Andy Dickinson	**Version issue date**	03/09/2013

Privacy Impact Assessment; Functions of the Health and Social Care Information Centre

Copyright ©2013 Health and Social Care Information Centre

Document Management

Revision History

Version	Date	Summary of Changes
1.0	12 April 2011	Original report
1.1	28 June 2013	1st draft revision for internal review
1.2	4 July 2013	Further draft for internal review
1.3	23 July 2013	Draft for wider internal review
1.4	1 Aug 2013	Draft including HSCIC Exec Team updates. Final draft subject to ratification.
1.5	6 Aug 2013	Further draft incorporating Comms Team changes
1.6	9 Aug 2013	Final draft incorporating reviewers changes (Comms, GPES, Care.Data)
1.7	20 Aug 2013	Version for consideration of Exec Board
2.0	3 Sept 2013	Final

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Paul Newton	IG Subject Matter Expert, HSCIC	23 July 2013	1.3
HSCIC Executive Team		26 July 2013	1.3
Clare Sanderson	Director of Information Assurance, HSCIC	23 July 2013	1.5
Katherine Guerin	Communications Team, HSCIC	8 August 2013	1.5
Kristina Wilcock	HSCIC Press Office	8 August 2013	1.5

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
Clare Sanderson		Director of Information Assurance, HSCIC	3 Sept 2013	2.0

Glossary of Terms

Term / Abbreviation	What it stands for
See Appendix B; “Glossary of terms”	

Copyright ©2013 Health and Social Care Information Centre

Document Control:

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Copyright ©2013 Health and Social Care Information Centre

Contents

Copyright ©2013 Health and Social Care Information Centre

1 Executive Summary

This privacy impact assessment relates to the overarching responsibilities of the Health and Social Care Information Centre (HSCIC). An Executive Non-Departmental Public Body (ENDPB), the Health and Social Care Information Centre was established in April 2013 as an independent organisation with important statutory duties, as set out in the Health and Social Care Act (2012).

A privacy impact assessment is a methodology to identify, assess, mitigate or avoid privacy risks. It describes the functions of the organisation to enable the reader to assess for themselves what may be considered a potential impact on their privacy, but it also goes on to explain what the organisation will do to protect individuals' privacy, and to identify solutions.

The Health and Social Care Information Centre collects analyses and publishes national data and statistical information, which are used to inform decision-making and patient choice. It also manages national IT systems and services to support the health and care system. These information services and products are used extensively by a range of organisations to support the commissioning and delivery of health and care services. The patient, and therefore protecting patient confidentiality, is at the heart of everything we do.

While the Health and Social Care Information Centre is a new organisation, there is continuity in many of its functions inherited from predecessor organisations, including safe and secure processing of data. In relation to privacy, the main change relates to powers the Health and Social Care Information Centre has under the Health and Social Care Act to collect and process patient identifiable data.

1.1 How the Health and Social Care Information Centre protects personal information

The Act provides powers for the Health and Social Care Information Centre to be the focal point for collecting, storing and disseminating national data from health and social care bodies. To do this it;

- collects centrally approved data and has the power to require a health or social care body to provide information
- can consider requests from other arm's length bodies for data to be collected
- publishes non-identifiable data, in standard and aggregated formats, for wider use by a wide variety of customers and to inform patient choice.
- helps with developing understanding of data and improving its robustness and quality.

The Health and Social Care Information Centre also has a duty to seek to reduce the administrative burden of data collections in the NHS.

Like all organisations that process and store patient identifiable data, the Health and Social Care Information Centre must protect the confidentiality of that data and guard against risks and threats from inside and outside the organisation.

The public must have confidence in the way information is collected, analysed and published. It is important that they are fully aware of these arrangements and how to exercise autonomy as individuals in the use of their information.

To safeguard the information it uses the Health and Social Care Information Centre has the following range of controls to mitigate the risks;

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

- Obtain and process only the minimum necessary patient identifiable data from other organisations:
- Store and process identifiable data securely, meeting or exceeding the standards required of NHS organisations, including processes and technology to:
    - de-identify data received as early as possible, and where records have to be linked, separate patient identifying data from clinical data, and assign a meaningless identifier[1]
    - store data in its capacity as the "safe haven", under the Health and Social Care Act (2012)
    - protect against attacks from unauthorised individuals (e.g. hackers)
    - protect against inappropriate behaviour by staff;
    - provide only legitimate personnel with access to the Health and Social Care Information Centre systems, and no more access than they legitimately require;
- Keep to the absolute minimum the number of staff able to access and view patient identifiable data, and wherever practicable assign staff rights of access to either patient identifiers or clinical data but not both;
- Destroy data held in identifiable form as soon as it is no longer required, or in accordance with the retention policy;
- Disclose only anonymised data, other than:
    - with explicit patient consent;
    - where *required* by law, or
    - where *allowed* by law, with necessary support and approvals, and through either:
        - the support of an Independent Advisory Group; or
        - where urgent, with the agreement of both the Senior Information Risk Owner and Caldicott Guardian for the Health and Social Care Information Centre;
- When disclosing anonymised data, restrict the data disclosed according to the context in which the data will be used:
    - when publishing statistics and other aggregated information, apply disclosure control standards[2] to ensure data are anonymised;
    - when disclosing patient-level data to a trusted organisation:
        - confirm the data are anonymised by carrying out a risk assessment
        - maintain a written agreement with the recipient organisation that stipulates the permitted access to, and uses of, the data;
- Monitor who accesses patient identifiable data.

[1] This process, known as "pseudonymisation", is a standard privacy-enhancing technique.

[2] The Health and Social Care Information Centre's current policy is available at: http://www.ic.nhs.uk/webfiles/publications/NHS_IC_Statistical_Governance_Policy_v2.pdf

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

Further Information Governance measures will also be put in place including:

- a review of the fitness for purpose of cyber security policies, processes and controls.
- upholding standards required to be the “safe haven” for storing data, as set out in Health and Social Care Act 2012

The Health and Social Care Information Centre will also be held to account against a number of pledges designed to protect information about patients;

- Publish a Code of Practice to govern the use of confidential data supplied to the Health and Social Care Information Centre;
- Act on patient objections to the Health and Social Care Information Centre using their data (unless there is a statutory duty or an overriding public interest (e.g. public health emergency) to do otherwise);
- Commission, at least annually, external information assurance audit against information governance standards.
- Be transparent about its activities and communicate openly, fairly and lawfully through its public website and other channels where appropriate;
- Publish procedures for dealing with requests for information and operate effective policies and procedures to encourage good information governance by staff, with proportionate sanctions (e.g. dismissal) for inappropriate or negligent behaviour.

1.2 Maintenance of the privacy impact assessment

The Health and Social Care Information Centre aims to fulfil its statutory roles and functions efficiently and effectively, maintaining high quality delivery of national services and products, and supporting the design and delivery of new information programmes. Protection of privacy is fundamental to all that we do. Given the constantly changing environment, this privacy impact assessment will be reviewed regularly.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

2 Introduction

2.1 The purpose of a privacy impact assessment

Privacy impact assessments were launched in the UK by the Information Commissioner in December 2007, and mandated by the Cabinet Office for Information and Communications Technology (ICT) projects following the Data Handling Review of June 2008[3].

A privacy impact assessment (PIA) should be seen as a dynamic process, taking into account current legislation, policies and organisational structures, and to that end the Health and Social Care Information Centre PIA will be reviewed regularly. In particular, this version acknowledges future policy may be shaped by the imminent Government response to Dame Fiona Caldicott's report; "Information; To Share Or Not To Share? The Information Governance Review".

The scope of this privacy impact assessment is intended to cover overarching Health and Social Care Information Centre functions. These include data flows such as the Data Services for Commissioners, the Care.Data programme and General Practice Extraction Service (GPES) programme, which are referred to by way of example later in this section. In instances where specific privacy issues are introduced through the collection of personal data, a separate PIA will be carried out.

The Health and Social Care Act introduced legislative powers that enable the Health and Social Care Information Centre to collect, and where necessary store, patient identifiable data extracted from patient records, which can occur without the consent of the individual in exceptional circumstances, but with the means to make an objection.

Patients and those legally empowered to act on their behalf[4] should be informed about how identifiable data is used and how they can object if they so wish.

The Health and Social Care Information Centre aims to ensure that patients are informed about its functions and how these relate to the protection of personal data. This privacy impact assessment will:-

- Describe the functions of the Health and Social Care Information Centre;
- Assess the potential implications for privacy, and;
- Explain what the Health and Social Care Information Centre is doing to protect privacy.

We welcome feedback on this privacy impact assessment upon publication.

2.2 The Health and Social Care Information Centre

The Health and Social Care Information Centre plays a fundamental role in driving better care, better services and better outcomes for patients, by;

- providing key services that support commissioning and reimbursement, including Casemix, the Quality Outcomes Framework (QOF) the GPES, and the Data Service for Commissioners.
- establishing and operating systems for the collection or analysis of certain information, on receiving direction from the Secretary of State or NHS England. To

[3] http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf

[4] This includes those with parental responsibility for children lacking competence, and people with lasting power of attorney acting for patients lacking mental capacity.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

fulfil our obligations we may require organisations to supply information, including in specific circumstances identifiable information.

- making data available in accessible formats that encourage use, such as machine readable formats and statistical reports, and by the development of resources such as an Indicator Portal, which brings data and methodological details from several sources into one, central place.
- helping people understand the robustness of the information they are using, through data quality and indicator assurance functions
- supporting commissioning and use of information standards by helping commissioners deliver on their obligations for the publishing of standards, and supporting care services to apply consistent and robust practices locally, to improve outcomes through more comprehensive and more consistent use of information.

In addition, the Health and Social Care Information Centre will :-

- deliver national IT systems and services to support the health and care system.
- maintain the critical national infrastructure that supports care delivery - including the Spine, NHSMail, the N3 network, Electronic Prescribing, Choices, Choose and Book, Summary Care Record and Local Service Provider delivered systems
- provide professional software development, support and hosting resources for the Health and Social Care Information Centre and the wider NHS
- approve and accredit local and national IT systems against technical and clinical safety standards and deliver a suite of in house systems and services
- ensure the proper management of our information assets, including the protection of individual privacy
- respond to the wider government agenda to increase the transparency and availability of public data.

2.3 Processing Personal Information

In April 2011 the Government consulted widely on issues including:-

- Improving quality in the NHS
- Ensuring patient involvement and public accountability
- Education and training to support modernisation
- Seeking advice from all healthcare professions to improve patient care

This “pause, listen and respond” initiative provided stakeholder feedback for the resulting Health and Social Care Bill (now Act).

As a result of this consultation, powers were included in the Act to allow the Health and Social Care Information Centre to obtain and process information extracted from patient records, which in some circumstances may impact on individuals’ privacy.

The following section uses examples of larger Health and Social Care Information Centre services and programmes to demonstrate information flows that are subject to this PIA, which will be equally applicable to most Health and Social Care Information Centre services and programmes. In instances where specific privacy issues are introduced through the collection of personal data, a separate PIA will be carried out.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

2.3.1 Data Services for Commissioners

The Data Service for Commissioners is a new service that processes data to support local commissioning whilst protecting patient confidentiality. NHS England has commissioned the Health and Social Care Information Centre to deliver this service. Staff seconded into the Health and Social Care Information Centre from Commissioning Support Units (CSUs) will deliver the service. Seconded staff continue to work from their local offices using regional processing centres.

The service will receive and process personal information on behalf of Commissioning Support Units (CSUs) and Clinical Commissioning Groups (CCGs). This will reduce or remove the need for these organisations to handle personal information and allow them to deliver focus on their core commissioning functions.

The Health and Social Care Information Centre is authorised to securely provide personal information where there is a lawful basis to do so, such as for direct patient care, where patient consent has been given or if approval has been given by the Secretary of State for Health under section 251 approval.

Patients receive care in different care settings from different health professionals, all of whom record the care and treatment given. This means information about patient care is recorded in a number of different places. In order to plan and organise care treatment, commissioners must be able to view all the treatment a patient receives. Personal information is needed, such as NHS number, date of birth, gender and postcode to ensure the right information is matched to the right person to give a true picture of care.

After information has been securely linked within the DSC the identifiers such as the NHS number, date of birth, gender and postcode can be removed before that information is shared with Commissioning Support Units (CSUs), NHS England Area Teams and Local Authorities.

2.3.2 GPES

The General Practice Extraction Service (GPES) is a centrally managed primary care data extraction service that will, for the first time, extract information from GP IT systems for a range of purposes at a national level.

GPES is part of the new process to provide payments to GPs and clinical commissioning groups. GPES will extract data from GP clinical systems to support payments to GPs and pass this to the Calculating Quality Reporting Service who will calculate the payments.

By improving access to primary care data for the NHS and other approved organisations, GPES will support a diverse range of services and initiatives that aim to improve the diagnosis, treatment and prevention of illness.

Confidentiality and security of patient data is of paramount importance which is why GPES has established Information Governance principles. These have been approved by the National Information Governance Board and also by the Medical Ethics Committees of the British Medical Association and the Royal College of GPs[5].

In order to safeguard patient confidentiality and maintain data security, potential GPES customers are required to undergo an approvals process to use the service, demonstrating how they plan to use the data they have requested and how that data will be used to provide benefits and improved care and outcomes for patients.

[5] See; “GPES IG Principles”; http://www.hscic.gov.uk/media/1532/GPES-IG-Principles/pdf/GPES_IG_Principles_0312.pdf

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

The GPES approvals process includes the consideration of extract requests by an Independent Advisory Group (IAG) that includes members of the public and representatives from General Practice.

2.3.3 Care.data

Care.data is a service that has been commissioned by NHS England and will be delivered by the Health and Social Care Information Centre. Care.data will make increased use of information from records across health and social care with the intention of improving healthcare and outcomes for patients, for example by ensuring that timely and accurate data are made available to:

- NHS commissioners and providers so that they can better design integrated services for patients,
- help the NHS plan ahead for public health emergencies,
- provide researchers with information they can study to find better ways to prevent illness and treat conditions.

As an initial stage in the programme, the Health and Social Care Information Centre will link data extracted from GP systems with data from other health and social care settings. Data about patients will be used for the linkage to ensure that the right records relating to the right patients are matched together. Once the data has been linked together it will only be shared with commissioners, providers and researchers where there is a lawful basis and appropriate approvals in place to do so.

The data will be extracted from GP systems monthly from late 2013 via the GPES. Extractions will be based on four groups of data; patient demographics, events, referrals and prescriptions, and the GPES Independent Advisory Group has recommended that these extractions should proceed and be made available in a way that does not identify any person or individual. Any changes to this extraction will be subject to further IAG consideration.

2.4 Balancing public interest and privacy

This document considers the balance between the need to protect patient privacy and the need to process data in the public interest. For example, there may be in instances where secure processing of patient record data will protect public health and improve patient care.

This section identifies potential benefits of the Health and Social Care Information Centre's functions using data extracted from patient records. The main benefits are achieved from informing the public, future health and care services, and the government.

2.4.1 Informing the public

The government wants to drive forward an “information revolution” in the NHS. The general public has a central role in this revolution;

- Patients will be more involved in making decisions about their own health and care, improving outcomes and reducing costs.
- Patient choice will reward the most efficient, high quality services, reducing expenditure on less efficient care.
- The NHS information revolution will also lead to more efficient ways of providing care, such as on-line consultations. Greater transparency will make it easier to compare the performance of commissioners and providers.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

Liberating the NHS: An information strategy lists the kinds of information that people will use, including[6]:

- suitable medicines, treatments, and any risks, benefits and side effects;
- clinical outcomes and success rates, such as readmission or mortality rates;
- other indicators of quality and performance, such as infection rates.

An important role of the Health and Social Care Information Centre is to provide such information, enabling patients to make informed choices and play their part in making a more effective, efficient health service. The Health and Social Care Information Centre must be proactive, encouraging people to make use of information we publish. We must also be responsive; providing appropriate information, subject to appropriate information governance controls.

2.4.2 Informing future healthcare services

The Health and Social Care Information Centre will also provide information to enable research, public health surveillance, clinical audit and other important purposes that are fundamental to improving health care. This can best be illustrated by an example. Consider a patient with lung cancer attending a hospital out-patient clinic in order to receive chemotherapy. The patient's treatment relies upon use of patient-related data for a host of medical purposes including:

- Decades of research into the most effective interventions for that form of cancer, including:
    - Clinical trials of each constituent drug in the group of drugs they are receiving in that chemotherapy regime, and each of the sub-optimal alternative drugs not being used, so that results and side-effects can be identified,
    - Clinical trials into different combinations of potential drugs, in different doses, administered in different frequencies through different methods in order to test potential chemotherapy regimes,
    - "Desk-based research" to assess evidence from around the world of outcomes of clinical trials and actual treatment using different chemotherapy regimes;
- National clinical audit to assess the provision of cancer care[7];
- Review of patient-reported experiences to identify how the provision of care can improve outcomes;
- Reporting to the Health Protection Agency through the "yellow card scheme" of adverse reactions of other lung cancer patients to chemotherapy regimes;
- Analysis by the National Patient Safety Agency of cases of misdiagnosis of lung cancer;
- Surveillance by local authorities and other public health agencies to identify high-risk target groups that might benefit most from "stop smoking" campaigns, and assess different methods of conveying the public health message effectively;
- Work by commissioning organisations to assess, commission and monitor the chemotherapy service provided by the acute trust;

[6] See *Liberating the NHS: An information strategy* available at: https://www.gov.uk/government/publications/liberating-the-nhs-white-paper

[7] Such as the National Lung Cancer Audit - see: http://www.hscic.gov.uk/lung

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

- Inspection of the acute trust and its services by the Care Quality Commission;
- Responses by the trust to previous complaints from patients receiving lung cancer services;
- Review of trust performance figures by the GP referring the patient; and
- Review by the acute trust oncology service manager of previous out-patient clinic appointment lengths for similar patients to plan and schedule the timings and skill-mix required for appointments in the clinic; and
- Reporting and monitoring of waiting times to meet targets for cancer patients.

Whilst none of the above activities involves the care of an individual patient, they are all fundamental to the lung cancer patient's care. All depend upon access to anonymised data derived from confidential information in patient records. A major role of the Health and Social Care Information Centre will be to provide such information.

2.4.3 Informing Government

A vast amount of data are collected and submitted centrally and the government has asked the Health and Social Care Information Centre to review and eliminate returns of limited value. Nevertheless, good information is essential to effective policy: it relies on high quality, timely information about what health services are provided, and the quality, effectiveness and efficiency of those services. The Health and Social Care Information Centre has a central role in providing this information.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

3 The Potential Impact on Privacy

3.1 Introduction

This section assesses the potential impact on privacy of the Health and Social Care Information Centre functions outlined above. Safeguards to protect privacy are explained in Section 4.

The main potential impact on privacy results from using data extracted from patient records. Functions carried out by the Health and Social Care Information Centre include the requirement to:

I. collect, and where necessary store, patient identifiable data extracted from patient records, which can occur without the consent of the individual in exceptional circumstances, but with the means to make an objection;

II. assure the quality of patient identifiable data, which may require patient identifiable data to be viewed;

III. link and de-identify patient identifiable data;

IV. publish and in some circumstances, disseminate anonymised data to specific bodies;

V. where necessary, in exceptional circumstances and with lawful authority, disseminate patient identifiable data to specific bodies.

These five cases are discussed below. In each case, the privacy impact is considered and the need for the processing is explained.

3.2 Processing patient identifiable data securely

The Health and Social Care Information Centre, like all organisations that process and store patient identifiable data, must protect the confidentiality of that data and must guard against risks and threats from inside and outside the organisation.

Recognising the increasing impact of "cyberspace" the Government also acknowledge new threats that come with it and have committed to a 2015 target to make the UK the safest place in the world to do business in cyberspace and to be more resilient to cyber attacks.

The UK Cyber Security Strategy "Protecting and Promoting the UK in a Digital World"[8] goes on to say;

> *"While cyberspace fosters open markets and open societies, this very openness can also make us more vulnerable to those – criminals, hackers, foreign intelligence services – who want to harm us by compromising or damaging our critical data and systems. The impacts are already being felt and will grow as our reliance on cyberspace grows".*

The Health and Social Care Information Centre is conducting a review of the fitness for purpose of the policies, processes and controls placed around health and social care data to ensure that it is secure amid increasing concerns about information assurance and cyber security.

[8] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

There have been a number of surveys of public attitudes to use of patient records and privacy risks[9]. One such study by the Royal College of Engineering led to the publication of *Privacy and prejudice: young people's views on the development and use of electronic patient records*. Most of the concerns reported were about privacy and the risk of data "getting into the wrong hands"[10]:

> "The "wrong hands" include those who might gain access by illegal means (for example, by hacking, fraudulent activity or coercion) in addition to those who might be given 'official access' by the EPR regulators." [Note: "EPR regulators" means the bodies in control of the electronic patient records.]
>
> "The set of organisations that made up the 'wrong hands' were commercial companies, 'private' companies, organisations that wanted to sell your data, advertising agencies, insurance companies, employers or potential employers, the media and in some cases, the Government."
>
> "The Government itself could be considered a pair of 'wrong hands' with questions raised over whether it would have access and therefore would be able to misuse or exploit the data".

Thus, key public concerns, which are likely to apply to all health records held and processed by public agencies such as the Health and Social Care Information Centre, are:

- the risk of data being accessed illegally and then sold or otherwise misused by commercial organisations, criminals or others; and
- the risk of data being accessed legally and then the data being misused.

Potential types of misuse are wider than articulated in the Royal College report. For example, data could be accidentally or purposefully changed, deleted, otherwise corrupted or lost.

However, misuse from illegal access, and misuse from legal access provide two helpful and legitimate headings for understanding risk. Although, as with any risk, these risks can never be eliminated completely, they can be addressed and minimised by effective and robust information governance controls (see section 4).

3.3 Collecting and storing data about patients

The Health and Social Care Information Centre is defined under the Health and Social Care Act 2012, which establishes it as a 'safe haven' with powers to collect and analyse confidential information about patients.

This means the organisation has been entrusted by the Government to be the place where data collected about health and social care patients and services users can be analysed for purposes other than the direct provision of care, such as identifying overall trends in health or shaping services to deliver better care in the future.

Some of this information is confidential data, meaning that details such as names, NHS numbers, postcodes or other identifiers may be included and must be held securely.

The table below sets out some reasons for collecting and storing confidential data, the potential impact that may have on their privacy and the controls to mitigate impacts.

[9] See: DH Paper; "Liberating the NHS; No decision about me, without me" https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/156256/Liberating-the-NHS-No-decision-about-me-without-me-Government-response.pdf.pdf

[10] See section 5.8 of the report, available at: http://www.raeng.org.uk/news/publications/list/reports/Privacy_and_Prejudice_EPR_views.pdf

Reason for processing and benefits	Impact on privacy	Controls and Pledges
• Data collected are fundamental to the operation of the NHS, and/or necessary to improving public health or health services. • Patient identifiable data is necessary for specific programmes of research. It is not practicable to gain consent for the data disclosure when millions of records are submitted on a routine basis (e.g. for Hospital Episode Statistics records). • In some cases (but not all), omitting individual records would affect the accuracy of Hospital Episode Statistics records, for example.	• Data storage and processing creates risk of confidential information being accessed without knowledge or consent of patients • Some people may feel a loss of individual autonomy (no patient consent)	• Statutory basis for data collection required by law • Identifiable data must be necessary to satisfy the purpose • Identifiable data stored only where necessary and destroyed or anonymised as soon as no longer necessary • Controls 1, 2, 3, 4, 7 – (see Section 4.2 – “Information Governance Controls”) • Pledges A, B, C, D & E – (see section 4.3 – “Additional pledges to protect information”)

3.3.1 The right to object

Patients have a right to object to personal information about them being collected and used by the Health and Social Care Information Centre – see Section 4.3 “Additional Health and Social Care Information Centre pledges to protect information”.

The Health and Social Care Information Centre will take account of patients’ objections but in very exceptional circumstances we may have to override objections and collect information from all patient records. Such circumstances would depend on there being an overwhelming public interest, such as a public health emergency where a contagious disease has broken out and accurate information is needed to protect the public. To date this has never actually happened.

This does not override the statutory duty to respect the patient opt out if section 10 of the Data Protection Act is invoked, for example, when processing is likely to cause substantial damage or distress.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

3.3.2 Assuring data quality

Usually checking data accuracy (and exceptionally, resolving computer system problems) can be done automatically using computer software. However, sometimes errors can only be identified and resolved by people accessing and viewing identifiable or non-identifiable data.

The following table shows the reasons for collecting and sharing patient identifiable data without the consent of patients, the potential impact on privacy, and the controls to mitigate the impact on privacy.

Reason for processing and benefits	**Impact on privacy**	**Controls and Pledges**
• Information used by the public to make health care decisions, and by people inside and outside the NHS for activities such as medical research, public health and national clinical audit, has to be of a good quality. The Health and Social Care Information Centre is responsible for assuring this. • Accuracy has to be checked before data are de-identified (it is not possible afterwards)	• Potential risk of confidential information being accessed without knowledge or consent of patient • Some people may feel a loss of individual autonomy (no patient consent)	• Controls 2, 3, 4, 7 – (see Section 4.2 – “Information Governance Controls”) • Pledges B, C, D & E - (see section 4.3 – “Additional pledges to protect information”)

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

3.3.3 Linking and de-identifying patient identifiable data

Linkage involves matching together two or more records about the same patient to provide a fuller picture of patient health characteristics and needs. For example, hospital records and general practice records about diabetic patients could be linked in order to assess whether patients are receiving appropriate care. De-identification typically involves removing identifiers (like name and address) and removing or changing other data items (e.g. changing date of birth into age). Alternatively, it could involve aggregating data (e.g. calculating the total number of patients in England receiving a hip replacement, broken down by age). De-identifying data is a fundamental means of protecting confidentiality.

Reason for processing and benefits	Impact on privacy	Controls and Pledges
• Once data are de-identified it can be used without breaching confidentiality for a large number of "secondary purposes" that are fundamental to the operation of the NHS and/or necessary to improving public health or health services. • Linking together two records about a patient is a powerful means of increasing knowledge and is used, for example, in medical research, public health and national clinical audit. It can also be used for direct care purposes e.g. linking data from general practice and hospital records to enable practices to invite patients at risk of heart failure and emergency hospital admission to be screened by a specialist nurse.	• De-identifying data reduces or eliminates the risk of a person's identity being revealed and thus protects privacy • Some people may feel a loss of individual autonomy (no patient consent)	• Controls 1, 2, 3, 4, 7 – (see Section 4.2 – "Information Governance Controls") • Pledges B, C, D & E - (See section 4.3 – "Additional pledges to protect information")

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

3.3.4 Publishing and disseminating anonymised data

Organisations must seek to achieve the balance between laws that protect patient confidentially and those that relate to public interest and transparency. Human Rights and Data Protection legislation, along with our domestic common law duty to respect confidentiality, require us to protect information that could identify an individual. In contrast, the Freedom of Information Act requires public authorities to release information about their activities, while the Health and Social Care Act allows the Health and Social Care Information Centre to obtain and disseminate information.

Transforming identifiable data into anonymised data protects personal privacy and enables published information to be used for public benefit. But although the law makes a clear distinction between identifiable and non-identifiable data, the line between the two requires scrutiny and consideration, often on a case by case basis.

The Health and Social Care Information Centre Information Standards Board (ISB) has published an anonymisation standard to ensure health and social care organisations can securely transform data that identifies individuals into data that is anonymised. This process standard[11] provides an agreed and standardised approach, grounded in the law, enabling organisations to:

- Distinguish between identifying and non-identifying information
- Deploy a standard approach and a set of standard tools to anonymise information to ensure that, as far as it is reasonably practicable to do so, information published does not identify individuals.

Reason for processing and benefits	Impact on privacy	Controls and Pledges
• The data output are fundamental to the operation of the NHS, and/or necessary to improving public health or health services and informing the public.	• In some cases, a small residual risk that identifiable data could be revealed • Risks may increase as more anonymised data are made available, and to more organisations (both public and non-public) • Some people may feel a loss of individual autonomy	• No constraints for use of published statistics or reports • Restrictions on re-use apply in other circumstances • Controls 2, 6, 7 – (see Section 4.2 – "Information Governance Controls") • Pledges A, B, C, D & E - (See section 4.3 – "Additional pledges to protect information")

[11] http://www.isb.nhs.uk/library/standard/128 Ref ISB 1523 "Anonymisation Standard for Publishing Health and Social Care Data"

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

3.3.5 Disseminating patient identifiable data (in exceptional circumstances)

The Health and Social Care Information Centre will not disclose patient identifiable data to other organisations other than in exceptional circumstances. The Health and Social Care Act does not provide the Health and Social Care Information Centre with any special powers to disclose patient identifiable data. To be lawful, explicit patient consent, approval under section 251 of the NHS Act 2006 or some other statutory authority will be required.

Reason for processing and benefits	Impact on privacy	Controls and Pledges
• There may be specific reasons for the Health and Social Care Information Centre to provide identifiable data to other organisations, but each case must be legally justifiable.	• Some people may feel a loss of individual autonomy (unless done with explicit patient consent)	• Disclosure must be lawful[12] • Controls 1, 2, 3, 4, 5, 7 – (see Section 4.2 – "Information Governance Controls") • Pledges A, B, C, D & E - (See section 4.3 – "Additional pledges to protect information")

3.4 Conclusions

A potential positive impact of the functions of the Health and Social Care Information Centre is that more organisations should be able to make use of anonymised information provided by the Health and Social Care Information Centre rather than using identifiable information.

The potential risks to privacy from the functions of the Health and Social Care Information Centre are:

A. Loss of individual autonomy from use of patient identifiable data without consent

B. Risk of confidential information being accessed and viewed without the knowledge or consent of patients

C. Linking and de-identification processes may not be reliable enough to achieve total anonymisation of data

D. Risk of data being accessed illegally and then sold or otherwise misused by commercial organisations, criminals or others; and

E. Risk of data being accessed legally and then the data being misused.

The actual impact on privacy will be mitigated by a full range of controls which the Health and Social Care Information Centre will use to safeguard the identifiable information it uses – discussed in section 4.

[12] The Health and Social Care Information Centre has no special powers to disclose patient identifiable data under the Health and Social Care Act. Should this ever be necessary, it must be lawful and justifiable either through explicit patient consent, section 251 of the NHS Act 2006, statute or the public interest.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

4 What will the Health and Social Care Information Centre do to Protect Privacy?

4.1 Introduction

This section explains what the Health and Social Care Information Centre will do in order to safeguard patient privacy.

The Health and Social Care Information Centre has been processing patient records safely and securely since its inception. It has introduced strong security controls, published and implemented security policies and published information about its processing as required for compliance with the Department of Health's Information Governance Framework.

The Health & Social Care Information Centre takes its responsibilities as a custodian of patient information extremely seriously and is also committing to a number of pledges to protect privacy as set out below (see 4.3).

A table in Appendix B shows how the privacy risks identified in section 3 are addressed by the information governance controls and pledges below.

4.2 Information Governance Controls

The Health and Social Care Information Centre provides assurances regarding Information Governance through:-

- an Information Assurance Steering Group, with reporting lines to the Executive Board
- satisfactory completion of the NHS Information Governance Toolkit[13], and compliance with ISO27001/2 Information Security Standards, which include:
    - Staff training and contracts
    - information technology system security and audit trails
    - Robust management arrangements
    - Full compliance with legislative requirements.
    - Provision of the "safe haven" for sensitive information

Specifically, the Health and Social Care Information Centre will:-

1) **Obtain and process only the minimum necessary patient identifiable data from other organisations:**
2) **Store and process identifiable data securely, meeting or exceeding the standards required of NHS organisations, including processes and technology to:**
    i. **De-identify data received as early as possible, and where records have to be linked, separate patient identifying data from clinical data, and assign a meaningless identifier (psuedonymisation).**
    ii. **Store data in its capacity as the "safe haven" under the Health and Social Care Act (2012)**
    iii. **protect against attacks from unauthorised individuals (e.g. hackers)**
    iv. **protect against inappropriate behaviour by staff;**

[13] See https://www.igt.connectingforhealth.nhs.uk/

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

v. provide only legitimate personnel with access to Health and Social Care Information Centre systems, and to no more access than they legitimately require;

3) Keep to the absolute minimum the number of staff able to access and view patient identifiable data, and wherever practicable assign staff rights of access to either patient identifiers or clinical data but not both;

4) Destroy data held in identifiable form as soon as it is no longer required, or in accordance with the retention policy;

5) Disclose only anonymised data, other than:

   i. With explicit patient consent;

   ii. where *required* by law, or

   iii. where *allowed* by law, with necessary support and approvals, and either:

   - the support of an Independent Advisory Group; or
   - where urgent, with the agreement of both the Senior Information Risk Owner and Caldicott Guardian for the Health and Social Care Information Centre;

6) When disclosing anonymised data, restrict the data disclosed according to the context in which the data will be used:

   i. When publishing statistics and other aggregated information, apply disclosure control standards[14] to ensure data are anonymised;

   ii. When disclosing patient-level data to a trusted organisation:

   - confirm the data are anonymised by carrying out a risk assessment
   - maintain a written agreement with the recipient organisation that stipulates the permitted access to, and uses of, the data;

7) Monitor who accesses patient identifiable data.

4.3 Additional Health and Social Care Information Centre pledges to protect information

In addition to the information governance best practice outlined above, the Health and Social Care Information Centre will put further safeguards in place to protect information and will be held to account against these pledges by the Department of Health. The Health and Social Care Information Centre will:

A. Publish a Code of Practice to govern the use of confidential data supplied to the Health and Social Care Information Centre;

B. Act on patient objections to the Health and Social Care Information Centre using their data (unless there is a statutory duty or an overriding public interest (e.g. public health emergency) to do otherwise);

C. Commission, at least annually, external information governance audit against information governance standards.

[14] The Health and Social Care Information Centre's current policy is available at: http://www.hscic.gov.uk/media/1350/Publications-Calendar-Statistical-Governance-Policy/pdf/The_HSCIC_Statistical_Governance_Policy_v3.1.pdf

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

D. Be transparent about its activities and communicate openly, fairly and lawfully through its public website and other channels where appropriate;

E. Publish procedures for dealing with requests for information and operate effective policies and procedures to encourage good information governance by staff, with proportionate sanctions (e.g. dismissal) for inappropriate or negligent behaviour.

5 Conclusions

The functions of the Health and Social Care Information Centre to collect, analyse and publish national data and statistical information must be augmented by protecting the confidentiality of that data and guarding against risks and threats from inside and outside the organisation.

Its information services are used extensively by a range of organisations to support the commissioning and delivery of health and care services, which are used to inform decision-making and patient choice. But the public must have confidence in the way information is used. It is important that they are fully aware of arrangements to exercise their autonomy as individuals in the use of their information. The Health and Social Care Information Centre will respect patient objections to the use of their data (unless there is a statutory duty or an overriding public interest (e.g. public health emergency) to do otherwise).

Some people may believe that any use of patient identifiable data without explicit patient consent is unacceptable. These people are unlikely to be supportive of the Health and Social Care Information Centre's functions whatever the potential benefits. Even people who feel the impact will be detrimental to privacy may recognise that the potential benefits of the Health and Social Care Information Centre using data from patient records are great, and may feel they are justifiable ethically on that basis. Those who conclude that the net impact on privacy will be positive are very likely to be supportive of the functions of the Health and Social Care Information Centre.

The Health and Social Care Information Centre has a range of controls to safeguard the information it uses and to mitigate risks. It is committed to meeting or exceeding all information governance standards, providing greater assurance than most organisations are able to provide. But there is also a positive impact on privacy resulting from the Health and Social Care Information Centre de-identifying data which can then be used more widely. Making anonymised or de-identified data available to researchers, public health specialists, clinical auditors and others eliminates their risk of inappropriate use of identifiable data.

While the Health and Social Care Information Centre is new, its functions, including the safe and secure processing of data, are well founded, tried and tested in previous constituent organisations. The patient, and therefore protecting patient confidentiality, is at the heart of everything we do.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

Appendix A - Managing Privacy Risk

A (i) - Types of privacy risk

The Information Commissioner's Office Privacy Impact Assessment Handbook explains why privacy matters and identifies and describes four classes of privacy risk:

- privacy of personal information;
- privacy of the person;
- privacy of personal behaviour; and
- privacy of personal communications.

The Health and Social Care Information Centre's functions could potentially pose risks to the privacy of personal information i.e. the first of the bullets above.

Two categories of risk to the privacy of personal information are relevant:

A. Risks to individuals as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information;

B. Risks to organisations providing and/or using the Health and Social Care Information Centre with data as a result of:

   I. perceived harm to privacy;

   II. a failure to meet public expectations on the protection of personal information (causing damage to the organisation's reputation);

   III. failure to comply with the law, leading to enforcement action from the Information Commissioner; or compensation claims from individuals.

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

A(ii) - Risk Mitigation Matrix

This section identifies a list of potential privacy risks and potential impacts, with corresponding information governance controls and pledges to reduce the risks to privacy. The table below indicates which risks each of the pledges is intended to address.

Control/Pledge to reduce risk/impact	Loss of autonomy	Confidential information viewed without consent	Misuse following illegal access	Misuse following lawful access
1) Obtain the minimum necessary identifiable data	√	√		
2) Store and process identifiable data securely		√	√	√
3) Minimise staff able to view identifiable data	√	√		√
4) Destroy identifiable data when no longer necessary	√	√	√	
5) Disclose only anonymised data (other than lawful exceptions)	√	√		√
6) Restrict the data disclosed according to context e.g. whether or not published	√	√		
7) Monitor who accesses patient identifiable data		√		
A. Establish an Independent Advisory Group		√	√	√
B. Maintain agreements with data suppliers			√	√
C. Respect patient opt outs	√	√		
D. Commission information governance audits		√	√	√
E. Be transparent and communicate fairly and lawfully	√	√		
F. Operate good information governance amongst staff with sanctions for misconduct		√	√	√

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

Appendix B - Glossary of terms

This document uses a variety of terms of particular relevance to privacy, and which could be open to more than one interpretation. To avoid the risk of misinterpretation, the table below contains a set of definitions. Wherever possible, it relies on existing published definitions, and in particular those in the Data Protection Act 1998, Section 251 of the NHS Act 2006[15] and in *Confidentiality: NHS Code of Practice 2003*[16] Where a definition is a partial extract from a lengthy published definition, the convention "…" is used below to denote this.

Term	Definition (or extract from full published definition)	Source
Aggregate data	Data derived from records about more than one person, and expressed in summary form, such as statistical tables.	Anonymisation Standard for Publishing Health and Social Care Data Specification
Anonymisation	Any processing that minimises the likelihood that a data set will identify individuals. A wide variety of anonymisation techniques can be used; some examples of such processing are explained in this specification. Also commonly referred to as "de-identification".	Anonymisation Standard for Publishing Health and Social Care Data Specification
Clinical Audit	The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services.	Confidentiality: NHS Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
Confidential patient information	"….patient information is "confidential patient information" where— (a) the identity of the individual in question is ascertainable— (i) from that information, or (ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and (b) that information was obtained or generated by a person who, in the circumstances, owed an obligation	Section 251 of the NHS Act 2006

[15] Available at: http://www.opsi.gov.uk/acts/acts2006/ukpga_20060041_en_19

[16] Available at: http://www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/DH_4069253

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

	of confidence to that individual.”	
De-identifying data	Any processing that minimises the likelihood that a data set will identify individuals. A wide variety of anonymisation techniques can be used; some examples of such processing are explained in this specification. Also commonly referred to as “anonymisation”.	Anonymisation Standard for Publishing Health and Social Care Data Specification
Explicit consent	“This means articulated patient agreement. A clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.”	Confidentiality: NHS Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
Identifiable information	A set of information from which a person (or persons) can be identified. Identifiable information is confidential, and so the definition for confidential patient information above also applies. Identifiable information can take a variety of forms, such as full patient records, extracts from records, and information not typically considered a record such as labelled laboratory samples.	Confidentiality: NHS Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
Information governance	Information Governance is to do with the way organisations ‘process’ or handle information. It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records.	Information Governance Framework Standard http://www.isb.nhs.uk/library/standard/121
Patient identifiable data	Key identifiable information includes: • patient’s name, address, full post code, date of birth; • pictures, photographs, videos, audio-tapes or other images of patients; • NHS number and local patient identifiable codes; • anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.	Confidentiality: NHS Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
personal data	“Data which relate to a living individual who can be identified:- - from those data; or - from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the	Data Protection Act

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

	individual”.	
processing	“Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including – - organisation, adaptation or alteration of the information or data; - retrieval, consultation or use of the information or data (which, in relation to personal data, includes using the information contained in the data); - disclosure of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available, or - alignment, combination, blocking, erasure or destruction of the information or data.” Note that a very similar definition for “processing” is used within the NHS Act 2006.	Data Protection Act
Pseudonym-isation	A technique that replaces identifiers with a pseudonym that uniquely identifies a person. In practice, pseudonymisation is typically combined with other anonymisation techniques.	Anonymisation Standard for Publishing Health and Social Care Data Specification
public interest	“Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.”	Confidentiality: NHS Code of Practice
safe haven	A bounded secure environment suitable for the receipt, storage, transmission and other processing of any confidential information, including the most sensitive personal information. It may be a physical space (such as a secure room), a configuration of electronic devices or a combination of the two, where secure processes are enforced.	
secondary uses service	SUS is primarily a data warehouse that provides access to anonymous patient-based data for purposes other than direct clinical care.	SUS Programme
Section 251 (or	Refers to Section 251 of the National Health Service Act 2006. It provides the power to ensure	NHS Information Governance –

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.

s251)	that patient-identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can only be used to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice.	Guidance on Legal and Professional Obligations - DH/Digital Information Policy Sept. 2007
sensitive personal data	The Act defines categories of sensitive personal data, namely, "personal data consisting of information as to:- (a) the racial or ethnic origin of the data subject; (b) his political opinions; (c) his religious beliefs or other beliefs of a similar nature; (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); (e) his physical or mental health or condition; (f) his sexual life; (g) the commission or alleged commission by him of any offence; or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."	Data Protection Act

Copyright © 2013. The Health and Social Care Information Centre All rights reserved.