Type 1 objections and the National Data Opt-Out

RCGP Position Statement

OCTOBER 2019

EXECUTIVE SUMMARY

The Department of Health and Social Care proposes to publish a plan to withdraw the type 1 objections after consultation with the National Data Guardian. The Royal College of General Practitioners (RCGP) proposes that the NHS implements plans to minimise the impact of this withdrawal on patient data choices and minimise the use of confidential patient information for purposes beyond individual care.

Type 1 objections recorded in GP records represent patients' choice to opt out of their confidential patient information being used for purposes beyond their individual care without their explicit consent. The objection applies to flows of data under the Health and Social Care Act (2012), section 259. The latest figures available from NHS Digital (March 2018) show that 2,085,450 people in England had type 1 objections, with numbers slowly increasing every year. The Department of Health and Social Care's current proposal is to replace type 1 objections with the single national data opt-out at some point after March 2020.

The third Caldicott Review, "Review of Data Security, Consent and Opt-Out" (2016) recommended that the national data opt-out should not be applied to data flows required under the law, such as the Health and Social Care Act (2012). This could lead to an unacceptable loss of patient autonomy and an increase in the flow of confidential patient information from GP practices for purposes beyond the patient's individual care without patients' consent.

The RCGP recommends that eight steps be taken by the NHS before type 1 objections are withdrawn:

1. General practice is technologically enabled to implement the national data opt-out when processing confidential patient information for purposes beyond individual care and meet their legal duty to report to their patients on how they have processed confidential patient information about them for such purposes.
2. Use of the NHS number as the single unique strong identifier in patient records is mandated for by all health and social care organisations and it is used as the single encrypted identifier for linking patient-level datasets to minimise the requirement for confidential patient information for purposes beyond individual care.
3. Robust de-identification-at-source systems that remove, blur or pseudonymise patient-level data before it is released by health and social care organisations are implemented in GP computer systems to minimise the risk that de-identified patient-level data released by data controllers may be re-identified.
4. Access to any confidential patient information should only be allowed for purposes beyond individual care when it is not possible to achieve the approved purpose of the data access with de-identified data.
5. Where the release of confidential patient information by the source organisation is necessary, the recipient must protect the confidential patient information to minimise the risk of a privacy breach and de-identified the data as soon as personal data is no longer necessary. This should be a standard requirement or data sharing agreements.
6. Following implementation of the preceding steps, the collection of confidential patient information for purposes beyond individual care by NHS Digital will be minimised, especially where the Health and Social Care Act (2012), section 259 provides the legal justification for access to the data and the national data opt-out does not apply. and all processing of confidential patient information by NHS Digital must be transparent and in line with clinical ethical standards.
7. Patients with an existing type 1 objection and a national data opt-out will automatically be credited with a single national data opt-out that all health and social care organisations will observe. Patients must not be expected to re-register their opt-out.
8. Before the type 1 objections are withdrawn, general practices must be fully informed about the impact of the change on data flows from practices and their responsibilities to inform patients about how they may object to data flows.

GLOSSARY

Confidential patient information: identifies the person that it relates to, says something about their health, care or treatment and is information that patients would expect to be kept private and for which GP practices have a duty of confidentiality.

Secondary purposes / secondary uses: this is an abbreviation which means purposes beyond a patient's individual direct care. They include medical research and NHS planning and management and many other purposes such as legal, employment, insurance and commercial purposes.

Type 1 objection: recorded in GP health records at the request of patients who want to prevent all confidential patient information being shared outside their GP practice for purposes other than individual care i.e. all secondary purposes above.

Type 2 objection: These no longer exist, but they prevented confidential patient information being released by NHS Digital for purposes beyond the individual's direct care i.e. the type 2 opt-out was replaced by the National Data Opt-Out in May 2018.

National Data Opt-Out: introduced in May 2018, following recommendations from the National Data Guardian. People can opt out of having their confidential patient information shared for reasons beyond their individual care, for example for research and planning. This is not held at the GP surgery but is held centrally. GPs cannot see if a patient as a national data opt out currently, but they still hold the Type 1 objection.

Other opt-outs: there are other opt-outs in the health system, which this proposal does not relate to, including:

- **Summary Care Record**: An opt-out is available for those patients that do not want to have a Summary Care Record. This confidential patient information is shared for individual care and type 1 objections and the national data opt-out do not apply.
- **Cancer registry**: The National Cancer Registration and Analysis Service, which is part of Public Health England, collects information about every cancer patient in England. If a patient does not opt-out of the cancer registry but does opt-out of the national data opt-out, the cancer registry will currently still be able to collect confidential patient information about them, but it will not share it beyond the registry.
- **National Congenital Anomalies and Rare Diseases Registration Service**: This also has a separate opt-out. Data will not be shared from this registry if the patient has a national data opt-out.

Patient-level data: data that is presented as a table where each row relates to a different individual.

De-identified data: patient-level data from which personal identifiers such as name, address, date of birth, NHS number have been stripped out or replaced by a coded reference or pseudonym that cannot be traced back to an individual patient, to create a dataset where no personal identifiers are present. It may be possible to trace data back to the individual it relates to if the data can be compared successfully with data from another source (a so-called "jigsaw attack") or if the pseudonym identifier can be linked to an individual (for example by reversing the encryption).

Anonymous information: data that cannot be traced back to an individual. It is not personal data. The information may be aggregated where the data is presented as totals, in the form of statistics or trends, which are rarely possible to trace data back to individuals. It may also be patient-level data to which privacy enhancing techniques such as de-identification, pseudonymisation or blurring of data have been applied. If such data is protected so that the risk that the data may be re-identified is negligible it may be considered anonymous.

Whether data may be considered anonymous is assessed according to the Information Commissioner's Office's "Anonymisation, Managing Data Protection Risk: Code of Practice". The national data opt-out policy does not apply to anonymous information.

Pseudonymisation: is one process that can be used to anonymise data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified. The pseudonym may be derived by encrypting one of more strong identifiers such as the NHS number. Pseudonymisation is one of the techniques that can be used to enhance the privacy of data.

BACKGROUND

Access to high quality data is vital to enable medical research and planning to take place. Wherever possible, patient data should be fully anonymised before it is used for research and planning, to reduce the need for sharing of any confidential or identifiable information and thus to reduce the requirement to seek individual patient consent or use legal routes to access data without consent.

Type 1 objections (type 1 opt-outs) were introduced, in part to enable patients to object to any confidential patient information about them being extracted from their GP records (with a few legally mandated exceptions), following the concerns raised by the attempted introduction of care.data.

Type 2 objections (type 2 opt-outs) were introduced to enable patients to object to any of their data leaving the GP surgery for reasons other than their individual care. These have subsequently been replaced by the National Data Opt-out and are not the focus on this paper.

Type 1 Objections

Type 1 objections / opt-outs were introduced in England in 2013 as government policy by the Secretary of State in response to public and professional concern about care.data[1,2] and the restriction of citizen's rights to object to the use and sharing of their confidential patient information under the Health and Social Care Act (2012), section 259. It also applied to the existing NHS Act (2006), section 251.

This paper focusses on the 'secondary use' of confidential patient information in England i.e. use of data for reasons other than the individual's direct care including research of all types, planning, management, legal, employment and insurance purposes – state and commercial. The combination of legislation and government policy on patient rights to object or opt-out of the use of confidential patient information about them for purposes beyond their individual care in England do not apply to Scotland, Wales or Northern Ireland.

Processing confidential patient information for purposes beyond individual care such as medical research, NHS planning, commercial, employment or legal purposes without explicit consent from the patient requires a legal basis for setting aside the common law duty of confidentiality.

A Read/SNOMED CT code recorded in the GP record establishes that a patient has made a type 1 objection. The latest figures available in 2018 showed that 2,085,450 people had a type 1 objection, with numbers slowly increasing every year.

The type 1 objection codes can be used to exclude patients with a type 1 objection in their GP record from searches run on data in computer systems. A few well-established research projects have specific consent codes that can be used where patients want confidential patient information to be used for specific research projects.

General practices are the only health and social care organisations that have the technology to record or implement a patient's objection to confidential patient information about them being processed for purposes beyond individual care. This problem was foreseen, and type 2 objections were introduced as the best available solution to prevent the release of confidential patient information by NHS Digital where patients objected.

National data opt-out and type 2 objections

The single national data opt-out was introduced by the government in response to the recommendations of the third Caldicott Review, "Review of Data Security, Consent and Opt-Out" (2016)[3], to simplify patient's choices about their data by replacing the two existing objections with one opt-out in due course. All health and social care organisations are currently required to implement the national data opt-out by March 2020, including primary care networks and local health and care record organisations.

All type 2 objections held by NHS Digital were simultaneously withdrawn and transformed into national data opt-outs in May 2018. NHS Digital maintains records on who has a national data opt-out on the Spine[4] this information is not recorded in GP records.

Patients have been able to set their national data opt-out online since May 2018[5] or by using the NHS App. The latest data from NHS Digital reports that 1,639,012 patients had national data opt-outs in May 2019[6].

Type 1 objections are still active and should continue to be implemented by general practices until a decision is made and publicised widely to withdraw them[7].

The Department of Health and Social Care, in consultation with the National Data Guardian will bring forward proposals in March 2020 or sometime afterwards, to replace the type 1 objections[8].

IMPLEMENTING THE NATIONAL DATA OPT-OUT

General practices do not have a record of who has a national data opt-out, so they will not be able to directly exclude patients with a national data opt-out from searches and data extractions for purposes beyond individual care if current systems continue. NHS Digital have stated that they intend to commission systems that will enable health and social care organisations to obtain a list of patients with a national data opt-out recorded on the Spine to exclude them from confidential patient information releases.

Currently GPs can only use a system supplied by NHS Digital called MESH, which is a laborious process[9]. NHS Digital plans for GPs to use a similar, less burdensome system but it is not clear if this will definitely be included in the GP IT Futures framework, nor is it clear if GPs will be able to report to patients on their processing of confidential patient information as required by GDPR, article 15[10] although the Department of Health and Social Care has promised that this will be possible by March 2020[8].

THE IMPACT OF CHANGING TO A SINGLE NATIONAL DATA OPT-OUT

The government response to third Caldicott Review stated that type 1 objections will be withdrawn at some point on or after March 2020 and replaced by the national data opt-out[8].

The current Department of Health and Social Care policy is that, unlike the type 1 objections, the national data opt-out will not be applied to releases of confidential patient information where there is a mandatory legal basis, such as the Health and Social Care Act (2012), section 259. If type 1 objections are withdrawn and replaced by the national data opt-out, patient's will lose their right to object or opt-out of the use of their confidential patient information where the legal basis for access to confidential patient information is the Health and Social Care Act (2012) section 259. If the collection of confidential patient information by NHS Digital for new projects where the national data opt-out is not applied, there would be a risk of considerable professional and public protest[11,12,13,14,15,16].

In the past similar protests about information governance policy have contributed to the withdrawal or restriction of major NHS data projects and seriously damaged trust in the NHS as a protector of patient privacy.

The policy of the Department of Health and Social Care is that the national data opt-out will be applied where the legal basis is not mandatory. The most common example will be NHS Act (2006), section 251 where the Common Law Duty of Confidentiality can be set aside for approved the uses of confidential patient information for research and NHS planning[17]. The Human Research Authority's Confidentiality Advisory Group[18] is responsible for making recommendations about approvals of requests for access to confidential patient information for research and NHS planning. They maintain a register of approved schemes[19].

A credible plan to minimise the impact of the replacement of type 1 objections by the national data opt-out is needed. In particular it must minimise the use of confidential patient information for purposes beyond individual care where the legal basis is the Health and Social Care Act (2012), section 259.

RCGP POSITION

A combination of policy and technological solutions are outlined below which will enable the type 1 objections to be replaced by the national data opt-out with minimal impact on the frequency with which confidential patient information is used for purposes beyond individual care without the patient's explicit consent. A secondary goal is to minimise the need for the use of confidential patient information where the national data opt-out must be applied.

To achieve these goals, the below steps are needed to establish an effective system for managing the processing of confidential patient information for purposes beyond individual care and implementing the national data opt-out.

1 The withdrawal of type 1 objections should only take place after the following requirements have been met:

1.1 There is a suitable replacement for type 1 objections that enables patients to opt-out of the use of their confidential patient information for uses beyond the individual's direct care (this may be via the national data opt-out).

1.2 NHSX and NHS Digital have implemented a suite of changes to the processing of patient information by health and social care organisations that will minimise the use of confidential patient information for uses beyond individual care, in line with the principles of data protection by design and default.

1.3 NHSX and NHS Digital have implemented a suite of policies to ensure transparency and independent approval of applications for access to confidential or re-identifiable patient information that will foster trust where the use of confidential patient information is necessary.

2 These requirements may be deemed to have been met if NHSX and NHS Digital introduce the following (or equivalent) policy and technological changes:

2.1- General practice is technologically enabled to implement the national data opt-out in processing confidential patient information for purposes beyond individual care and meet their legal duty to report to their patients on how they have processed confidential patient information about them for such purposes.

All health and social care organisations must be able to comply with data protection legislation and their common law duty of confidentiality when they process confidential patient information. This includes being able to report to individual patients about specific releases of confidential patient information that relate to them. Yet NHS Digital is the only health and social care organisation that has a record of the identities of patients who have a national data opt-out. A general practice will not know which of their patients has a national data opt-out.

An efficient national service is needed which can assure that confidential patient information about patients with a national data opt-out is excluded from data releases by all health and social care organisations. The service must not place a new burden upon GPs. Organisations that are data controllers of confidential patient information must be able to answer patients' questions about whether their type 1 objections have been successfully converted to a national data opt-out and that their national data opt-out has been implemented.

2.2 - Use of the NHS number as the single unique strong identifier in patient records is mandated for by all health and social care organisations and it is used as the single encrypted identifier for linking patient-level datasets to minimise the requirement for confidential patient information for purposes beyond individual care.

Current data linkage protocols make use of postcodes, dates of birth and gender as well as the NHS number to increase the success rates of data linkage algorithms. Postcodes and gender identification can change with time causing errors in linkage and require the release of stronger identifiable information. Use of the NHS number alone, if it is present in every record and reconciled to a national service such as the Patient Demographic Service, should allow more accurate linkage and is amenable to pseudonymisation.

Work carried out by NHS Digital has shown that the NHS number can be successfully used on its own to link datasets where there are accurate records, reconciled to the Personal Demographic Service. The prevalence of accurate records in NHS organisations in England, Wales and the Isle of Man is high enough to allow very successful data linkage. Scotland and Northern Ireland use different unique identifiers. The Health and Social Care (Safety and Quality) Act 2015 mandates the use of a 'consistent identifier'. This is manifested in Regulations under the Health and Social Care Act (2012)[20].

NHS England's Five Year Forward View states that the NHS number "will be used in all settings including social care"[21], however its use by social care organisations is sporadic.

The universal use of a single system of unique strong identifier by all health and social care organisations would make it possible to link data from multiple sources with a very high degree of success, suitable for the great majority of purposes beyond individual care using the NHS number alone.

Note: Patient-level datasets are made up of one or more records where all the data about an individual patient are linked and usually labelled by a unique label, which may be a pseudonym or another identifier.

2.3 - Robust de-identification-at-source systems that remove, blur or pseudonymise patient-level data before it is released by health and social care organisations are implemented in GP computer systems to minimise the risk that de-identified patient-level data released by data controllers may be re-identified.

Encryption (or pseudonymisation) of the NHS number at source before it is released by the data controller, using a confidential, secure key and encryption algorithm replaces the NHS number in patient-level datasets with individual pseudonyms that are meaningless and impossible to link to a known individual without access to the algorithm and the key. It allows patient-level datasets to be linked without the need for sharing confidential patient information.

NHS Digital has procured encryption services for its own use and for other health and social care organisations[22]. Where NHS Digital controls and has access to the algorithms and keys used by health and social care organisations, data held by NHS Digital, where the identifiers are encrypted by them, must be considered to be personal data. NHS Digital has a statutory right to hold and process confidential patient information, which they may request from health and social care organisations using the Health and Social Care Act (2012) section 259.

Rich patient-level data without identifiable data may be re-identified. Even when a dataset contains no identifiers it may still be possible to re-identify an individual. Anyone with access to other personal data may be able to use it to identify an individual within a dataset (a so-called "jigsaw attack") where a known data pattern can be spotted in a data set, e.g. known events recorded on known days. Individual data to be released for purposes beyond individual care should be de-identified as thoroughly as possible before being released.

The use of de-identification-at-source may minimise the requirement for confidential patient information to be released and used for purposes beyond individual care. This reduces the risk of privacy breaches and will increase the confidence of health professionals and the public in how the NHS protects confidential patient information.

2.4 - Access to confidential patient information should only be allowed for uses beyond individual care when it is not possible to achieve the approved purpose of the data access with de-identified data.

NHS Digital has the statutory right to hold and process confidential patient information. It may also require health and social care organisations to release confidential patient information to it when directed under the Health and Social Care Act (2012) section 259, in which case the national data opt-out does not apply. To minimise the use of this power overriding patients' national data opt-out, confidential patient information can be de-identified before being released for purposes beyond individual care.

This should be the default practice although the risk of privacy breach in releasing confidential patient information for medical research and NHS planning must always be balanced against the potential public benefit from the use of the data.

2.5 - Where the release of confidential patient information by the source organisation is necessary, the confidential patient information must be protected by the recipient to minimise the risk of a privacy breach and de-identified by the recipient as soon as personal data is no longer necessary. This should be a standard requirement or data sharing agreements.

Approval for the use of confidential patient information for uses beyond individual care without explicit patient consent, relying on the Health and Social Care Act (2012) or the NHS Act (2006) as the legal basis must be independent and transparent and only given when it is impossible to achieve the reasonable aims of the data release with de-identified data. Data releases must comply with the General Data Protection Regulations (GDPR), the Data Protection Act (2018) and the Common Law Duty of Confidentiality. This should apply to the use and release of confidential patient information by all health and social care organisations, including NHS Digital.

Approval must ensure that the minimum confidential patient information is released to achieve the explicit aims of the purpose beyond individual care and that it is processed legally and fairly. The confidential patient information must be protected by a combination of technical and contractual arrangements to minimise the risk of a privacy breach and de-identified or destroyed by the recipient as soon personal information is no longer required. Data sharing agreements for confidential patient information should be in line with the requirements of the new NHSX Centre for Expertise guidance and standards[23].

Registers of confidential patient information released must be maintained to enable patients to know what confidential patient information has been shared with whom for which purposes beyond individual care to meet their rights under GDPR article 15[10].

Where access to confidential patient information is necessary for uses beyond individual care, alternatives to the release of confidential patient information should be used whenever possible so that only aggregate data or data robustly assessed to be ‘non-personal’ should be released to the secondary user:

1. Systems should be implemented that enable the data controller to carry out analyses on confidential patient information on behalf of the secondary user.
2. Alternatively, confidential patient information may be made available to the secondary user to carry out the analyses in a secure and protected environment such as NHS Digital’s Data Services Platform[24] and Data Access Environment[25]. Use of these services should enable NHS Digital to minimise the amount of confidential patient information it releases. Public Health England and other national providers of confidential patient information should adopt similar policies and systems.

2.6 - Following implementation of the preceding steps, the collection of confidential patient information for purposes beyond individual care by NHS Digital will be minimised, especially where the Health and Social Care Act (2012), section 259 provides the legal justification for access to the data and the national data opt-out does not apply. All processing of confidential patient information by NHS Digital must be transparent and in line with clinical ethical standards.

Practices are obliged to release confidential patient information to NHS Digital when the request is made under the Health and Social Care Act (2012), section 259. This has been used in the past to ensure that data is available from every practice, e.g. National Diabetes Audit was previously requested under the NHS Act (2006), section 251.

When a secondary purpose for patient-level information can be met with data that is de-identified at source, the Health and Social Care Act (2012) section 259, should not be used as a legal basis for releasing confidential patient information. Health and social care organisations should be obliged to

provide the de-identified data assuming that there is a suitable data sharing agreement that ensures that the recipient will protect the data to prevent any privacy breaches.

2.7 - Patients with an existing type 1 objection and a national data opt-out will automatically be credited with a single national data opt-out that all health and social care organisations will observe. Patients must not be expected to re-register their opt-out.

Most current national data opt-outs have been allocated to patients by transferring every type 2 objection held by NHS Digital to a national data opt-out (some have been set by patients online). This does not accurately represent the population with type 1 objections. There are patients who have requested a type 1 objection that do not have a national data opt-out. Their type 1 objections will have to be transferred to a national data opt-out held by NHS Digital, but it is not clear how NHS Digital will be able to do this. The problem is that the presence of a type 1 objection in a GP record currently prevents a GP sharing confidential patient information with NHS Digital for this purpose.

It seems reasonable that patients with a type 1 objection should not have to re-set their objection as a national data opt-out. A credible plan is needed to confidentially and automatically convert all type 1 objections to a national data opt-out where individuals do not already have a national data opt-out on the NHS Digital database.

2.8 - Before type 1 objections are withdrawn, general practices must be fully informed about the impact of the change on data flows from practices and their responsibilities to inform patients about how they may object to data flows.

Withdrawal of type 1 objections will have complicated effects on the flow of patient data from general practices. GPs will need to understand how to respond to requests for data including:

- Local flows to support individual care (e.g. primary care networks, integrated care services and local health and care records);
- Local flows to support health planning and research, including data flows to Data Services for Commissioners Reginal Offices (DSCRO)
- National flows under direction (mandatory flows) to NHS Digital;
- National flows to NHS Digital for payment purposes (via the GP Extraction Service or the Calculating Quality Reporting Service (CQRS));
- Other central collections of GP data (e.g. Clinical Practice Research Datalink (CPRD), QResearch, Apollo and other information intermediaries).

Details about the different ways that patients may object to confidential patient information being shared for purposes beyond their individual care must be clearly communicated, including national information campaigns. Information and educational support about how practices should implement opt-outs is also needed, including guidance around meeting responsibilities to fully inform their patients about how their confidential patient information is being used (e.g. type 1 objections, national data opt-out, the NHS Constitution[26] or GDPR).

Practices must be fully aware of instances when the common law duty of confidence has been set aside and patient objections are not being upheld.

REFERENCES

[1] The Independent Information Governance Oversight Panel's report to the care.data Programme Board on the care.data Pathfinder stage. (2014), https://www.gov.uk/government/publications/iigop-report-on-caredata (accessed on 6 August 2019)

[2] NHS to scrap single database of patients' medical details, The Guardian (2014) https://www.theguardian.com/technology/2016/jul/06/nhs-to-scrap-single-database-of-patients-medical-details (accessed on 6 August 2019)

[3] The third Caldicott Review, "Review of Data Security, Consent and Opt-Out" (2016) https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs (accessed on 6 August 2019)

[4] The Spine, introduction from NHS Digital, https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/ (accessed on 6 August 2019)

[5] Patients can register a national data opt-out via the NHS App or online at https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/ (accessed on 6 August 2019)

[6] [MI] National Data Opt-Out March 2019, NHS Digital, https://digital.nhs.uk/data-and-information/publications/statistical/national-data-opt-out/march-2019/ndop-mar19 (accessed on 6 August 2019

[7] Guidance for health and social care organisations on compliance with the national data opt-out, NHS Digital, https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out (accessed on 6 August 2019).

[8] The government response to the third Caldicott Review, "Your Data: Better Security, Better Choice, Better Care", Department of Health (2017) https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care (accessed on 6 August 2019)

[9] NHS Digital service to check for who has a national data opt-out from a list of NHS numbers sent by health and social care organisations to establish the records that can be used or disclose for NHS planning or research, NHS Digital, https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out/check-for-national-data-opt-outs-service (accessed on 6 August 2019)

[10] General Data Protection Regulation, European Union (2018), https://gdpr-info.eu/art-15-gdpr/ (accessed on 6 August 2019)

[11] "Patients need to have control over their own information if care.data is to work", The Guardian (2014) https://www.theguardian.com/healthcare-network/2014/feb/28/patients-need-control-information-care-data (accessed on 6 August 2019)

[12] "Care.data: how did it go so wrong", BBC News, (2014) https://www.bbc.co.uk/news/health-26259101 (accessed on 6 August 2019)

[13] The Independent Information Governance Oversight Panel's report to the care.data Programme Board on the care.data Pathfinder stage (2014) https://www.gov.uk/government/publications/iigop-report-on-caredata (accessed on 6 August 2019)

[14] "NHS England to re-brand 'toxic' Summary Care Record", Pulse (2013), http://www.pulsetoday.co.uk/your-practice/practice-topics/it/nhs-england-to-rebrand-toxic-summary-care-records/20004962.article (accessed on 6 August 2019).

[15] "Opting out of the NHS Spine", The Guardian (2010), https://www.theguardian.com/commentisfree/henryporter/2010/mar/02/nhs-spine-database-opting-out (accessed on 6 August 2019)

[16] "Patient experience surveys exempted from national data opt-outs", Digital Health (2019) https://www.digitalhealth.net/2019/01/patient-experience-surveys-exempted-national-data-opt-out/ (accessed on 6 August 2019)

[17] What is section 251? Health Research Authority, https://www.hra.nhs.uk/documents/223/cag-frequently-asked-questions-1.pdf (accessed on 6 August 2019)

[18] Health Research Authority Confidentiality Advisory Group, https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/ (accessed on 6 August 2019)

[19] Health Research Authority Confidentiality Advisory Group register of approved applications, https://www.hra.nhs.uk/planning-and-improving-research/application-summaries/confidentiality-advisory-group-registers/ (accessed on 6 August 2019)

[20] The Health and Social Care Act 2012 (Consistent Identifier) Regulations 2015, http://www.legislation.gov.uk/uksi/2015/1439/made (accessed on 6 August 2019)

[21] Five Year Forward Review, p32, NHS England (https://www.england.nhs.uk/wp-content/uploads/2014/10/5yfv-web.pdf (accessed on 6 August 2019)

[22] NHS Digital leading the protection of patient data with new patient de-identification solution, NHS Digital (2018) https://digital.nhs.uk/news-and-events/latest-news/nhs-digital-leading-the-protection-of-patient-data-with-new-patient-de-identification-solution (accessed on 6 August 2019)

[23] "NHS X to oversee data sharing agreements under new DHSC guidance", Digital Health (2019) (https://www.digitalhealth.net/2019/07/nhsx-to-oversee-data-sharing-agreements-under-new-dhsc-guidance/ (accessed on 6 August 2019)

[24] NHS Digital Data Services Platform, https://digital.nhs.uk/data-and-information/data-insights-and-statistics/improving-our-data-processing-services (accessed on 6 August 2019)

[25] NHS Digital Data Access Environment, https://digital.nhs.uk/services/data-access-environment-dae (accessed on 6 August 2019)

[26] NHS Constitution for England, https://www.gov.uk/government/publications/the-nhs-constitution-for-england (accessed on 6 August 2019)