15 October 2016

Terms and Conditions for the Storage and Use of Data for the National Maternity and Perinatal Audit

1.0 Organisations Sharing Data

Data will be shared between;

Royal College of Obstetricians and Gynaecologists (RCOG)
27 Sussex Place, Regent’s Park, London NW1 4RG.

And

University Hospitals of Bristol NHS Foundation Trust (hereafter referred to as the Participating Unit)

2.0 Purpose of Terms and Conditions

The RCOG’s Lindsay Stewart Centre for Audit and Clinical Informatics is conducting the National Maternity and Perinatal Audit (NMPA), commissioned by the Healthcare Quality Improvement Partnership (HQIP) on behalf of NHS England, the Welsh Government and the Health Department of the Scottish Government.

In order to conduct the NMPA, the RCOG requires certain patient-level maternity data from all NHS Trusts/Health Boards with a maternity service in England, Scotland and Wales. These Terms and Conditions refer to the release of that data, which is held on the Participating Unit’s electronic maternity record system(s) (or Maternity Information System(s), MIS), to the RCOG for the purposes of the NMPA.

3.0 Definitions

In these Terms and Conditions, the following words and phrases will have the following meanings:

Clean Database: the Database with the Patient Identifiers removed.

Data Extract(s): the patient-level maternity data from the Participating Unit (including Patient Identifiers) which is set out in Appendix 1.

Data Protection Legislation: the Data Protection Act 1998, as amended from time to time, and any superseding legislation including (but not limited to) Regulation EU 2016/679 (the “General Data Protection Regulation”), should it come into effect.

Data Protection Principles: the principles set out in the Data Protection Legislation, governing the processing of Personal Data.
**Database**: the database created by the RCOG which includes the data from maternity units across England, Scotland and Wales (including the Data Extract).

**HQIP**: Healthcare Quality Improvement Partnership.

**MIS**: Maternity Information System, or electronic maternity records system (the system used to record women’s clinical maternity information, for example relating to booking and labour/birth, in an electronic format).

**NMPA**: National Maternity and Perinatal Audit.

**NMPA Data**: any data processed by the RCOG for the purposes of the NMPA, including the Data Extract.

**NMPA Data Managers**: the two Data Managers for the NMPA (Appendix 2).

**Participating Unit**: University Hospitals of Bristol NHS Foundation Trust.

**Patient Identifier(s)**: the information contained in the Data Extract identifying individuals (for example the mother’s NHS number, date of birth or postcode).

**Permitted Parties**: the parties set out in Appendix 2, with access to the Database.

**Personal Data**: as defined in the Data Protection Legislation, and including Sensitive Personal Data.

**Sensitive Personal Data**: as defined in the Data Protection Legislation.

**SFTP**: Secure File Transfer Protocol.

### 4.0 Purpose of the NMPA

The Database is being established to enable the maternity data captured by NHS Trusts and Health Boards to be held securely in a central repository for the purposes of clinical audit and service evaluation. The NMPA will publish reports and will develop a web-based system to allow the Participating Unit to compare their maternity care and maternal/neonatal outcomes against national and regional figures.

To provide a rich set of information to the Participating Units, the NMPA will link the Database at an individual patient level to Hospital Episode Statistics (HES) and Office for National Statistics (ONS) data for English Trusts, and to Patient Episode Data for Wales (PEDW) and ONS data for Welsh Health Boards. This process will use the Data Linkage Service at NHS Digital and the NHS Wales Informatics Service (NWIS), respectively. Patient Identifiers contained within data extracts (including the Data Extract) will be securely transferred to NHS Digital and NWIS for linkage purposes.

To gain additional information, the NMPA will also link data extracts (including the Data Extract) at individual patient level to the following databases:

- The Intensive Care National Audit and Research Centre (for information on critical maternal care)
- The National Neonatal Audit Programme (for information on critical neonatal care)
- Public Health England’s surveillance systems SCSS and LabBase2 (for information on bloodstream infections)
- The English Mental Health and Learning Disabilities Data Set (for information on perinatal mental health)
In producing the information on patterns of care and local maternal and perinatal outcomes, the NMPA Data Managers will first remove Patient Identifiers from the Database to create the Clean Database. The Permitted Parties (Appendix 2) will then use the Clean Database for all analysis, to ensure patient confidentiality.

The primary outputs from the NMPA will be annual reports, online reports for individual providers, commissioners and networks, and reports of periodic time-limited, topic-specific audits. The NMPA may also produce conference presentations and peer-reviewed journal publications describing the methodological developments and overall findings of the NMPA. Results generated using the Clean Database may also be included in the PhD theses of some of the Permitted Parties. All results will be based on aggregated data to ensure patient confidentiality is preserved.

5.0 The RCOG’s Role and Responsibility

As the Data Processor, the RCOG will process all NMPA Data on behalf of the Data Controller, HQIP. As a Data Processor, the RCOG will act only in accordance with HQIP’s instructions and the RCOG’s agreement with HQIP.

The RCOG will hold all NMPA Data, in accordance with the provisions in paragraph 7 (Data Security and Retention) and in accordance with the Data Protection Principles. The RCOG has Section 251 approval from the Health Research Authority’s Confidentiality Advisory Group, on behalf of the Secretary of State, allowing handling of patient identifiable data without consent and linkage to other relevant datasets.

The RCOG will limit access to the data extracts to the NMPA Data Managers. The NMPA Data Managers will process the Data Extract, as well as other data extracts supplied by maternity units, to create the Database. They will undertake the process of separating the Patient Identifiers contained within the Data Extract from patient health and treatment data, in order to create the Clean Database. The records belonging to the same individual will only be identified with a NMPA-derived unique anonymised label.

The NMPA Data Managers will securely transfer the Patient Identifiers to NHS Digital and NWIS (who already have permission to access Patient Identifiers) who will provide the data linkage with the HES/PEDW and ONS databases.

Once the Patient Identifiers have been removed, access to the Database will be restricted to the Permitted Parties, who will handle all processing of this data. No individual other than the Permitted Parties can access the Data under these Terms and Conditions. In the case of staff changes (including a change in the identity of the NMPA Data Managers), the RCOG will inform the Participating Unit of these changes prior to new staff members gaining access to the NMPA Data.

6.0 The Participating Unit’s Role and Responsibility

During the course of these Terms and Conditions, the Participating Unit will arrange for the secure transfer of the Data Extract(s) from its local MIS covering the following periods:
- 1st April 2014 to 31st March 2016, by 16th December 2016;
- 1st April 2016 to 31st March 2017, by 15th December 2017;

The Participating Unit will transfer each Data Extract to the NMPA securely and in an encrypted format.
Before transfer of each Data Extract, the Participating Unit will encrypt the Data Extract using a product that provides ‘256-bit AES encryption’ with a password length of 12 which includes a mixture of upper and lower case characters, numbers, and special characters. The password must be kept separate from the Data Extract.

The encrypted Data Extract will be transferred to the NMPA Data Managers at the RCOG using a SFTP, as described in Appendix 3.

The Participating Unit will be sent its username by e-mail. The password will be given to the Participating Unit by telephone only, following authentication of its username and the individual’s identity. The username must be stored separately from the password.

The Participating Unit will not share the password with any person outside the Participating Unit, other than the NMPA Data Managers, at any time.

In the case of staff changes, the Participating Unit will inform the RCOG of these changes prior to new staff members discussing any aspect of the NMPA Data with the Permitted Users.

7.0 Data Security and Retention

The RCOG formally wishes to acknowledge its explicit commitment to maintaining the confidentiality, safety, security and integrity of all confidential and sensitive data to which their organisation is privy, and which may be held under its guardianship.

The RCOG will hold the NMPA Data and the data extracts (including the Data Extract) on a secure server within the N3 network. The server is operated by the RCOG, and is leased to the RCOG by RedCentric. RedCentric have provided NHS network services for many years and are contracted under an agreement that guarantees secure data processing. Their accreditations for N3 hosting are:

- Information Governance Statement of Compliance (IGSoC)
- NHS Digital-accredited N3 ISP (Network Access Agreement 0740)
- Independent aggregator of IGSoC Version 13 with a score of 100%
- Code of Connection approval (3rd party N3 hosting provider onto the N3 network by NHS Digital)
- Compliant Commercial Third Party (NACS Code YGMAP)
- Accreditation to store patient data for and on behalf of the NHS
- The Reading and Harrogate data centres are PCI Compliant for physical hosting services
- ISO27001 and ISO9001 certification

Further details on data security are given in the RCOG System Level Security Policy Document for the RCOG Secure Server (copy available on request).

Encrypted back-ups of the RCOG’s Secure Server are undertaken on a regular basis and stored securely by RedCentric.

As the Data Controller for the purposes of the NMPA, the HQIP is responsible for responding to external requests for access to the Database. Each party agrees to submit to any such requests received by HQIP.

The Database will not be released to any other individual(s) or organisation(s), except with the formal written approval of HQIP.
Patient Identifiers held by the RCOG will be destroyed once data cleaning and linkage have been successfully performed. The Clean Database will be retained on the RCOG’s Secure Server, in line with the Data Protection Principles and in accordance with Data Protection Legislation. A copy of the Clean Database and final processed data will be securely transferred to, and retained by, HQIP as the Data Controller, in line with the Data Protection Principles and in accordance with Data Protection Legislation.

If the Data Extract (or any data contained within the Data Extract) is to be destroyed in accordance with these Terms and Conditions, the RCOG will ensure that, for any such data held by the RCOG, the data destruction is performed securely using file shredding software. Similarly, physical media will be destroyed using a high specification shredder with the functionality to irreversibly destroy the disk. All data will also be removed from any archives and back-ups. Confirmation that this has occurred will be given in writing to the Participating Unit.

8.0 Access to NMPA Data

The Database may only be used for the purposes of clinical audit, service evaluation and research related to these activities.

All users of the Database and/or the Data Extract (including the RCOG, the Participating Unit and HQIP) are obliged to fully comply with Data Protection Legislation, together with all other related and relevant legislation and Department of Health directives covering issues of data sharing and including:

- British (International) Standard ISO 27001;
- The Caldicott Report 1997;
- The Caldicott Review 2013;
- The Freedom of Information Act 2000;
- Section 251 of the Health and Social Care Act 2006;
- Confidentiality: NHS Code of Practice 2003;
- NHS Records Management Code of Practice (Part 1, 2006 & Part 2, 2009);
- The NHS Information Security Management Code of Practice 2007;
- The Computer Misuse Act 1990;
- The Electronic Communications Act 2000;
- The Copyright, Designs and Patents Act 1988;
- The Re-Use of Public Sector Information Regulations 2005;
- The Human Rights Act 1998;
- NHS Care Record Guarantee.

No contact may be made with any individual(s) that could be identified from the information supplied. Any reports, papers or statistical tables that are published or released to other organisations will protect the identity of individuals in accordance with current Office for National Statistics Disclosure Control of Health Statistics guidance [http://www.ons.gov.uk/ons/guide-method/best-practice/disclosure-control-of-health-statistics/index.html](http://www.ons.gov.uk/ons/guide-method/best-practice/disclosure-control-of-health-statistics/index.html)

9.0 General

The RCOG agrees to immediately report to the Participating Unit incidents of breach of any of these Terms and Conditions. In the event of the material breach of any of these Terms and
Conditions by the RCOG, the Participating Unit has the right to request the destruction of the Data Extract. Any cleaned data or Clean Database will be sent to the HQIP before its destruction.

The RCOG has the right to make changes to these Terms and Conditions so that they remain consistent with current data protection standards and legislation, as well as its overarching agreement with the HQIP, by notice in writing to the Participating Unit.

Each party shall be liable to the other for damages or costs of losses incurred by the other party where such cost, loss or damages are caused by its actions or omissions. Liability as between the parties is limited to actual damage suffered. The RCOG shall not be responsible to the Participating Unit provided that the Permitted Parties act in accordance with HQIP’s instructions and the RCOG’s agreement with HQIP.

Any notice or other communication required to be given to a party under or in connection with these Terms and Conditions shall be in writing and shall be delivered by hand or sent by e-mail, pre-paid first-class post or other next working day delivery service, to the address or e-mail address specified in this clause.

The contact details for service of a notice under these Terms and Conditions are as follows:

The RCOG:

(a) Address: 27 Sussex Place, Regent’s Park, London NW1 4RG.

(b) For the attention of: Sara Johnson, Executive Director of Quality and Knowledge, Royal College of Obstetricians and Gynaecologists

(c) E-mail address: sjohnson@rcog.org.uk

Participating Unit:

(d) For the attention of: Dr Jane Luker, University Hospitals Bristol NHS Foundation Trust Headquarters

(e) E-mail address: jane.luker@uhbristol.nhs.uk

Any personally delivered or e-mailed notice shall be deemed received on the day it was delivered or sent, if it was delivered or sent on a business day before 5:00pm, and otherwise on the next business day. Any notice sent by pre-paid first-class post or other next working day delivery service shall be deemed to have been received at 9:00am on the second business day after posting, or at the time recorded by the delivery service.

These Terms and Conditions shall be governed by the laws of England, and shall be subject to the jurisdiction of the court of England and Wales.
Appendix 1. Summary of data items for the NMPA

This is a summary of the data items required and a detailed data extract specification will follow shortly. This may include some items which are not listed below, but no additional patient identifiable data (e.g. mother’s name or address) will be requested.

**Demographic:** (This information is essential for both linkage and risk-adjustment)
- Mother’s NHS number
- Mother’s postcode
- Mother’s date of birth
- Mother’s ethnicity
- Father’s ethnicity
- Mother’s employment status
- Father’s employment status
- Baby’s NHS number
- Private maternity patient flag

**Obstetric history:** (This information is essential for risk-adjustment)
- Gravida
- Parity
- Previous caesarean sections
- Previous instrumental deliveries
- Previous stillbirth
- Previous preterm birth
- Previous low birthweight infant

**Antenatal Care:** (This information is essential for risk-adjustment)
- Date of last menstrual period
- Date of antenatal booking appointment
- Reason for late booking if applicable
- Gestation at booking
- Maternal weight and height at booking
- Smoking status, alcohol, and substance use at booking
- Mother’s first language English
- Complex social factors
- Mental health screening
- Support status of mother
- Confirmed estimated date of delivery (and method)
- Antenatal risk factors/complications/diagnoses
- Intended place of delivery

**Delivery:** (This information is essential for indicator construction, linkage and risk-adjustment)

**Mother**
- Date and time of admission for delivery/induction
- Actual place of birth
- Transfer in labour (and reason)
- Smoking status at delivery
- Number of infants this delivery
- Rupture of membranes time
- Labour onset
• Type of induction
• Reason for induction, if applicable
• Labour augmentation
• Time of onset of first stage
• Time of onset of second stage
• Time of end of third stage
• Delivery of placenta method
• Analgesia/pain relief in labour and delivery
• Category of senior person present at delivery
• Method of delivery
• Decision to deliver time, if applicable
• Reason for instrumental delivery, if applicable
• Reason for caesarean, if applicable
• Category of caesarean, if applicable
• Delivery in water
• Episiotomy
• Perineal tears
• Blood loss (ml)
• Maternal complications/diagnoses

**Baby**

• Date of birth
• Time of birth
• Birth order
• Presentation at birth
• Status at birth
• Type of stillbirth, if applicable
• Birth weight
• Gestational age in days
• Sex of baby
• Cord blood gases pH (venous)
• Cord blood gases pH (arterial)
• Apgar score at 1 minute
• Apgar score at 5 minutes
• Apgar score at 10 minutes
• First feed status
• Feeding status on discharge
• Skin to skin contact within 1 hour
• Date/time of Newborn Infant Physical examination
• Resuscitation method
• Level of neonatal care
• Date/time admitted to neonatal care, if applicable
• Reason for admission to neonatal care
• Neonatal complications/diagnoses

**Discharge**: (This information is essential for the construction of indicators and for risk-adjustment)

• Date of maternal discharge
• Date of neonatal discharge
• Date of neonatal death, if applicable
• Date of maternal death, if applicable
## Appendix 2. Permitted Users

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMPA Methodological Lead</td>
</tr>
<tr>
<td>NMPA Methodological Advisor</td>
</tr>
<tr>
<td>NMPA Audit Lead</td>
</tr>
<tr>
<td>NMPA Data Manager</td>
</tr>
<tr>
<td>NMPA Data Manager/Statistician</td>
</tr>
<tr>
<td>Senior Clinical Lead (Obstetrics)</td>
</tr>
<tr>
<td>Senior Clinical Lead (Midwifery)</td>
</tr>
<tr>
<td>Senior Clinical Lead (Neonatology)</td>
</tr>
<tr>
<td>NMPA Clinical Fellow (Obstetrics)</td>
</tr>
<tr>
<td>NMPA Clinical Fellow (Midwifery)</td>
</tr>
<tr>
<td>NMPA Senior Methodologist</td>
</tr>
<tr>
<td>Lindsay Stewart Centre Manager</td>
</tr>
<tr>
<td>Lindsay Stewart Project Manager</td>
</tr>
</tbody>
</table>
Appendix 3. Instructions to Maternity Units for Data Transfer

Instructions for First Secure File Transfer for National Maternity and Perinatal Audit (NMPA)

Content and Timing of data transfer

The deadline for the first data transfer is Friday 16 December 2016.

You will be asked to send a single data extract of your electronic maternity record system containing the records of all maternity episodes resulting in:

Either

A birth (live birth or stillbirth) following 24 completed weeks of gestation

Or

A birth before 24 completed weeks of gestation where the baby showed signs of life.

The data extract should cover the 24 month period from 1st April 2014 to 31st March 2016.

A summary of the data items required is available in Appendix 1 and a detailed data extract specification will follow shortly.

The data items will be as closely aligned as possible with those required for the Maternity Systems Data Set (MSDS) from NHS Digital.

Please retain a copy of the data extract you send to us in case we have any queries regarding the data.

Method for data transfer

There are two possible methods of data transfer.

Method 1: Secure electronic file transfer

Please transfer the data to the NMPA secure server at the RCOG using a Secure File Transfer Protocol (SFTP) software, such as FileZilla. If necessary please see below for instruction on how to download and use FileZilla. Your allocated username will be sent to you via e-mail, along with the IP address and port for the data transfer. Please do not share the IP address or your username with any person other than the NMPA team at any time.

When you are intending to transfer the data to the secure server at the RCOG, please telephone the NMPA helpline using the telephone number given below. During the telephone call you will be asked to verify your name, the name of your Trust/Health Board and your username. You will then be given a password for the data transfer.

Please record the name of the member of the NMPA team you spoke to.

Please do not write down your password.

Method 2: Secure courier
Please use this method only if Method 1: Secure electronic file transfer is not possible. Please contact the NMPA team using the contact details below. You will be sent an approved, encrypted USB drive.

When you are intending to send the encrypted data, please telephone the NMPA helpline using the telephone number given below. During the telephone call you will be asked to verify your name, the name of your Trust/Health Board and your username. You will then be given a password for encrypting the data.

Please record the name of the member of the NMPA team you spoke to.

Please do not write down your password and do not share your password with any person other than the NMPA team at any time.

Please encrypt the data using a product that provides 256-bit AES encryption, such as 7-Zip, using the password you were given.

Please transfer the encrypted data onto this drive, and send it via secure courier to the NMPA team at the address below. Please use only the approved, encrypted USB drive provided by the NMPA, and no other type of disk, to send data.

Contact details for NMPA team

NMPA Data Transfer
Lindsay Stewart Centre
Royal College of Obstetricians and Gynaecologists
27 Sussex Place
Regent’s Park
London NW1 4RG

E-mail: nmpa@rcog.org.uk

NMPA helpline tel: 020 7772 6498

Changes to these instructions

The NMPA Data Manager will inform the trust contact of any changes to these instructions in writing prior to the changes taking place.

Changes to your details

In the case of changes to the details of our contact in your trust, please ensure that our current contact in your trust informs the NMPA Data Manager of these changes in writing prior to the changes taking place.
Instructions for Downloading and Using FileZilla for Secure File Transfer

Downloading FileZilla

FileZilla is free to download and you can do so as follows.

1. Click on the following link: https://filezilla-project.org/download.php or type it into your internet browser.
2. Click on the Download FileZilla Client button.
3. Click on the .exe file that appears at the bottom left hand side of the web browser window.
4. A window will appear asking if you want to run or save the file. Click Run.
5. If asked Are you sure? Click Yes.
6. You may be asked whether you wish to download additional software. Click Skip to avoid downloading other software.
   You will be taken through a series of questions for the FileZilla Client Setup. Follow the default options each time by clicking on Next.
7. You will be asked whether you would like to make FileZilla software available to all users of the system or just yourself. Click on your preferred option. Either is fine.
8. You will be asked where on your system FileZilla program files should be saved. Choose where you would like to save these files. An example of a suitable location is C:\Program Files\FileZilla FTP Client
9. You will be asked whether you agree with the FileZilla license terms and conditions. Once you have read and are happy with the agreement, click I Agree.
10. FileZilla will now be installed on your system.
Using FileZilla for Secure File Transfer

1. Start FileZilla
2. Enter the following details:
   a. Host: IP address
   b. Username
   c. Password
   d. Port: port number
3. Click on Quick Connect

4. The pane on the left-hand side of the window contains the files on your Trust/Health Board’s system,

while the pane on the right-hand side contains the files you have recently uploaded to the RCOG’s secure server.
Find the file to be transferred on your system and drag and drop it into the right-hand pane.

5. A copy of your file will now appear in the right-hand pane, showing that the file has been successfully transferred.