BMA

Guidance note: Template data sharing agreement and data processing agreement

General practice and PCN support

As part of the PCN DES, networks will need to have in place a relevant Data Sharing Agreement, to allow the sharing of data and information between members.

NHS England and the BMA have agreed on a, non-mandatory, high-level data sharing template for use by networks. To make things simpler for those practices and networks who may not have entered such an agreement before, the BMA has also produced a version of the agreed template, which expands on a number of areas within the template, and allows for the addition of more complete schedules within the agreement. This provides practices with a better idea of how they may wish to populate the template agreement, including proposed best practice when sharing and transferring data between partners within the network.

This note provides guidance to the expanded BMA draft Data Sharing Agreement, explaining the various sections and schedules within it. Whilst effort has been made to populate the template Agreement as much as possible, there are some sections which can only be completed by the PCN, with full knowledge of their specific operating structure and processes. Additional drafting notes are included within the relevant sections of the template Agreement to provide further guidance in these areas.

These documents were produced for the BMA by Mills and Reeve and practices should note that neither the BMA template nor this guidance constitute legal advice and are intended as a guide to be adapted as required. When completing the template Agreement it is recommended that practices receive professional advice in order to ensure that they are confident that the Agreement works for their PCN and that they are fully aware of all obligations under the Agreement and relevant data law.

Additional BMA guidance on information governance and data protection for GP practices can be found on the BMA website.

1 Differences between the templates

1.1 Expansion of Schedules – The BMA DSA expands Schedule 1 of the template DSA into separate schedules. This will allow PCNs to more accurately document the relationships between the PCN members including how data will be shared, what security measures the parties will need to implement and the appointment of shared processors (such as EMIS).

1.2 Removal of Consent Provisions – The BMA DSA has had the provisions relating to managing the consent of data subject removed as consent is not applicable for sharing personal data for direct healthcare purposes. However, it is possible that this could be applicable in some future situations if networks look to extend the sharing of personal data for purposes beyond healthcare provision. If practices wish to consider this, these can be found at clauses 3.11 and 3.12 of the joint DSA template.

1.3 Addition of Accession of New Party Provisions (clause 7) – The BMA DSA includes provisions that relate to the ability of the parties to allow a new member of a primary care network sign up to the data sharing agreement.

1.4 Addition of Voluntary Exit and Expulsion Provisions (clauses 8 and 9) – The BMA DSA includes provisions that relate provisions that allow a PCN member to voluntarily leave or be expelled from a primary care network to also leave the data sharing agreement.

1.5 Expansion of Certain Clauses – The BMA expands on the following clauses to increase the clarity of the obligations on the members of the PCN and assist PCNs in developing their data sharing arrangements:

1.5.1 Clause 3.8.2 – Security of processing;

1.5.2 Clause 3.12.2 – Complying with requests from other parties to amend personal data held by a party;

1.5.3 Clause 3.13.1-4 – Requirement to notify parties in the event of a breach of the data sharing agreement, data protection legislation or security breach;

1.5.4 Clause 3.16 – Requirement to rectify any security weaknesses reported to a party by another party;

1.5.5 Clause 5.3 – Requirements of processor agreements; and

1.5.6 Clause 6.2 and 6.3 – Requirements for each party's Privacy Notices.

Data sharing agreement

2 Scope and purposes of data sharing

2.1 The DSA is designed to enable each member of the PCN, as Parties to the agreement, via data sharing technologies (such as cloud-based Electronic Patient Record systems, or Electronic Data Interchanges), to:

2.1.1 make available to the other members Parties (where they have the same patient) the information contained in the patient records held by that Party, for the purposes stated in the Privacy Notice that the Parties have agreed to use, and the purposes are expected normally to be **only** for each Party to provide direct healthcare to the patient when called upon;

2.1.2 access the information contained in the patient records of the other Parties, for the purposes stated in the Privacy Notice that the Parties have agreed to use, and the purposes are expected normally to be **only** for each Party to provide direct healthcare to the patient when called upon; and

2.1.3 keep records about access to the shared patient data by each Party's staff, and audit the records.

3 Where to find information in the DSA

3.1 The DSA reflects the close relationship that exists between the Parties' purposes for using the data, and the legal grounds that they rely on (and which must be stated in the Privacy Notice that the Parties agree to use).

3.2 Schedule 1 contains the following information:

3.2.1 **paragraph 1 (Permitted Purposes)** states the specific scope of permission for each Party to use the shared data;

3.2.2 **paragraph 2 (Authorised Users)** states the specific staff roles, within each Party's organisation, that may be permitted to access and use the shared patient data (and this reflects the expectation that, normally, the Parties will only use shared patient data for the direct provision of healthcare, and will need to limit accordingly the staff roles who are able to access and use the data);

3.2.3 **paragraph 3 (Duration of the Processing)** records how long the Parties intend to continue sharing personal data (and, particularly if the Parties have different retention policies for personal data, this paragraph should also be used to define the retention periods that all of the Parties will consistently observe);

3.2.4 **paragraph 4 (Categories of Data Subject)** will state the specific categories of data subjects whose personal data will be shared (it is expected that normally this will be limited to patients, but some Primary Care Networks may wish to deploy Privacy Notices and governance so that they can include the sharing of certain personal data about their members' staff, as well);

3.2.5 **paragraph 5 (Categories of Personal Data)** will state, for each category of data subjects, the specific categories of personal data that will be shared;

3.2.6 **paragraph 6 (Legal bases for Processing)** will state the specific legal grounds that are relied on for sharing and using the shared personal data. The Parties will need to take independent legal advice on these if the purposes for use of the shared patient data are wider or different from the core purpose of the direct provision of healthcare, or if the categories of data subjects whose personal data is to be shared includes more than just patients;

3.2.7 **paragraph 7 (Confidentiality Compliance)** will set out how each party will ensure that disclosing the shared personal data does not breach confidentiality as required by clause 3.10;

3.2.8 **paragraph 8 (Additional Terms)** will state any additional obligations, on one or all of the Parties, which the Parties wish to include in the DSA in accordance with clause 11;

3.2.9 **paragraph 9 (Data Protection Contact)** will state the contact details for each Party's data protection contact who is appointed in accordance with clause 3.5; and

3.2.10 **paragraph 10 (Review Date/Frequency)** will state the date and frequency at which the Parties will review the DSA in accordance with clause 12.

3.3 **Schedule 2 (Agreed Sharing Mechanisms)** will outline the technology that is used for data sharing.

3.4 **Schedule 3 (Security)** will outline the security measures that the Parties will implement and adhere to during the term of the DSA.

3.5 **Schedule 4 (Shared Processors)** will set out the details of any shared processors of the Parties. Note that, under the DSA, a Shared Processor is a processor who is appointed to process shared personal data for *all* of the Parties.

3.6 **Schedule 5 (Deed of Accession)** sets out the Deed of Accession that any new party to the DSA will need to sign to become a party to the DSA.

4 Future changes

4.1 Once the DSA has been signed by the Parties, they may wish to share more fields of patient personal data, and/or to use the data for a wider range of purposes in the future. To achieve this, the Parties will need to formally vary the DSA. To comply with Data Protection Legislation, before entering legal agreements the Parties would likely need to carry out a Privacy Impact Assessment.

4.2 The PCNA allows for Parties to leave and join a Primary Care Network, so we have included provisions in the DSA to reflect this:

4.2.1 Under the PCNA a Party can leave voluntarily (subject to approval and a managed transition) or can be expelled. In essence, on ceasing to be a Party to the PCNA, they shall also cease to be a Party to the DSA. The DSA imposes appropriate additional requirements to ensure that the data and IT implications of the Party's exit are managed.

4.2.2 A new Party can join by signing a Deed of Accession, as set out in Schedule 5 of the DSA. The new Party would need to be a user of the data sharing technology referred to in Schedule 2, prior to joining.

5 Summary of the DSA's other provisions

5.1 The following are the other key provisions of the DSA:

5.1.1 Each Party has two roles under the DSA. The first role is that of "**Disclosing Party**". A Party is a Disclosing Party in relation to medical records that are created by that Party's staff, and in relation to personal data about its own staff.

5.1.2 In the DSA, each Party, in its capacity as a Disclosing Party, agrees that it will routinely disclose to the other Parties the types of personal data that are described in Schedule 1, paragraph 5. This is documented in the DSA because, for each Party to effect the data sharing, it will need to know exactly which data fields its IT systems need to be set up to *share with* the other Parties, and exactly which data fields its staff can expect to be able to view as *received from* the other Parties.

5.1.3 To differentiate them, the other Parties are referred to as "**Receiving Parties**" in the DSA. That is the second role that each Party has. Each Party, in its capacity as a Receiving Party, will be permitted to access the Disclosing Party's shared personal data for the purposes set out in Schedule 1, paragraph 1.

5.1.4 It is recommended that each Party, in its capacity as a Receiving Party, is contractually limited to only permitting certain of its staff to access and use the shared personal data. The categories of staff are described in Schedule 1, paragraph 2. If the purposes of the data sharing are limited to use of the data for the direct provision of healthcare, the categories of staff will be the staff whose job is the direct provision of healthcare, and other staff who are under the clinicians' direct supervision or who are responsible for the management of the direct provision of healthcare (albeit on a reduced access basis in the case of managers).

5.1.5 The DSA seeks to deal with IT and data security by explicitly providing checks and balances:

i. Each Party is required to implement and maintain IT and data security measures, to the basic standard that is set by Data Protection Legislation and by cyber-security laws).
ii. The DSA does not engage with the detail of security, because it is likely that no two Primary Care Networks will use exactly the same security measures. The DSA provides a space, in Schedule 3, where the Parties must describe the required security measures that must be maintained by the Primary Care Network in relation to data sharing and the electronic data sharing technology used.
iii. Each Party is required to take account of the data sharing, and the electronic data sharing technology (which should be described in more detail in Schedule 2) as part of its annual Data Security and Protection Toolkit self-assessment. The DSA also provides for each Party to review each other Party's Data Security Protection Toolkit.
iv. If there is a security breach affecting shared patient data, the DSA requires this to be notified very quickly to the other Parties.
v. Each Party is required to audit user logs in respect of its own staff.
vi. The DSA requires all Parties to keep the shared patient data in the EU unless the UK leaves the EU, in which case the shared personal data must be kept in the UK.

5.1.6 Each Party is required, for its own part, to comply with Data Protection Legislation, including ensuring it gives Privacy Notices to patients and staff, keeps appropriate records, keeps personal data secure and confidential, and appoints processors in compliance with the law. Any third party provider of the data sharing technology and/or supporting technologies must be appointed as a processor by a Party under its own contract with the IT provider (using an appropriate Data Processor Appointment agreement, **not** the Data Processing Agreement, which is not designed for use in this context).

5.1.7 There are no liability or indemnity provisions in the DSA to apportion liability amongst members of the PCN, or to indemnify respective members of the PCN, if they incur financial liabilities due a breach by a Party under the agreement. It's recommended that PCNs should take independent legal advice on these matters and if they decide to include such provisions, the DSA can be amended accordingly[a]. There are also no specific confidentiality provisions in the DSA. The Parties may already have in place Non-Disclosure Agreements with appropriate scope, before they discuss and enter into the DSA. If Non-Disclosure Agreements are not in place, the Parties should take independent legal advice and ensure that confidentiality provisions are included in the DSA.

5.1.8 The DSA is open-ended and is expressed as continuing in force until the PCNA is terminated. The DSA can be terminated if in the event there is only one Party left as a party to the DSA;

a In doing so practices should carefully consider how any such provisions operate and how any 'shared' liabilities will be apportioned, taking into account the requirements with the GDPR, and, in particular, setting out how Article 82 will be met in practice between the parties. This could be done, for example, by including indemnity in the agreement, so that (a) one party indemnifies the others if they incur liabilities due to the one party's breach, and (b) one party is indemnified by the others if it incurs liabilities that arise from a shared risk. Precisely how this such provisions are drafted will be dependent upon the operational practice of the PCN and the individual and collective decisions of the PCN participants based upon the professional advice received.

Data processing agreement

6 Scope and purpose of data processing

6.1 The Data Processing Agreement is intended to be entered into between two of the Parties, where one of them acts as a processor (processing certain shared personal data on behalf of the other Party, strictly to its instruction) for the other, who acts as a controller (who has lawful grounds to decide what purposes the data is used for).

6.2 In any scenario where a controller appoints a processor, the processor is required by law to be appointed by contract. The General Data Protection Regulation 2016/679 ("**GDPR**") prescribes what such contracts must cover. The DPA provides the basis for the controller and processor, in the scenario described in paragraph 6.1 above, to form a compliant contractual appointment. As with any legal instrument, the parties should take independent legal advice to ensure the agreement complies with GDPR.

6.3 The Parties will need to complete Annex 1 before signing the DPA. Annex 1 sets provides space for the Parties to describe:

6.3.1 the subject matter of the processing, which in this context might (for example) be the provision of certain hosting or other IT technical services;

6.3.2 the duration of the processing;

6.3.3 the nature and purposes for which the processor is appointed to process the shared personal data, i.e. broadly what it is required to do with the data, and any specific standing instructions;

6.3.4 the categories of data subject whose personal data will be processed; and

6.3.5 (for each category of data subject) the types of personal data that will be processed.

6.4 Annex 1 will need to be populated in detail. Under the DPA the processor is only permitted to process the personal data as set out in Annex 1 (unless any further written instructions are given subsequently by the Controller). If there are any discrepancies between the details in Annex 1 and the actual processing that the processor actually undertakes, that "gap" represents compliance risk for the controller and/or the processor.

6.5 As with the DSA, there are no liability or indemnity provisions in the DPA in the event of a breach by a Party to the DPA although the Parties may agree to include such provisions. If doing so it is recommended that they take legal advice in relation to liability.

6.6 The processing of the personal data under the DPA will only be required whilst the PCNA continues in force. The DPA is drafted to continue until either:

6.6.1 the PCNA expires or is terminated; or

6.6.2 either Party to the DPA ceases to be a Party to the PCNA (by reason of voluntary exit or expulsion).

6.7 There is also an optional provision for the controller to terminate the appointment of the processor on a months' notice.

British Medical Association
BMA House, Tavistock Square,
London WC1H 9JP
bma.org.uk

BMA 20190459