

KAFICO

— INFORMATION · GOVERNANCE · CONSULTANCY —

Version Control

Date	Notes	Author
August 2020	Initial Draft	Kafico Ltd

Sources

[Data Protection Act 2018 \(DPA\)](#)

[General Data Protection Regulations \(EU\) 2016/679 \(GDPR\)](#)

[Information Commissioner – Guide to the General Data Protection Regulations \(ICO Guide\)](#)

[ICO Guidance - Data Controllers](#)

[European Data Protection Board \(EDPB\) Opinion 00264/10/En Wp 169 \(WP29O\)](#)

[GDPR Lawful Processing - IGA](#)

[Control of Patient Information Notice](#)

1. Project Context

Medicines Management Solutions Ltd (MMS®) are a nationwide company who provide expert advice on all aspects of medicines management within Primary Care. MMS® have been providing pharmacist support to the NHS for over 10 years and have delivered support across over 2,000 sites nationwide.

For this particular project, MMS® will;

- review sub optimal or at risk non-anticoagulated patients
- highlight monitoring requirements and any inappropriate Direct Oral Anticoagulants (DOAC) dosing
- option to review warfarin patients in shielded criteria or Time in Therapeutic Range (TTR) <60%
- implement actions aligned with local DOAC formulary choice

KAFICO

— INFORMATION · GOVERNANCE · CONSULTANCY —

The Data Flows are;

1. MMS® provides appropriate assurances and pharmacist details for approval of remote working
2. GP lead highlights any special considerations relating to the scope of service
3. Prior to start, Pharmacist requires user rights & log in access to GP system, conduct searches, view letters and amend prescriptions this may include Docman & INR Star if used
4. HSCN/VPN secure remote notes-based review, screening for patients suitable for an intervention as per scope
5. Use NHSE warfarin and DOAC guidance to check metrics e.g. CHADVASC, CrCL, INR, indication and exclusion criteria such as valvular disease
6. Pharmacist shares recommendations with GP lead via secure NHS Mail and using traffic light system (Green appropriate/ Amber bloods due/ Red inappropriate)
7. Confirm GP approval for any changes to treatment plan
8. Patient telephone consultation to explain rationale for therapy change and share DOAC related advice
9. Implement and log any changes using appropriate templates and ensure read codes and therapy changes are recorded
10. Option for a patient list & template letter shared for surgery to distribute
11. Surgery to inform local pharmacies to further counsel patient on change to DOAC with potential for an NMS
12. Option for MMS® to follow up on patients up to 3 months post change to reassess notes and tele-consult as required

2. Controllers and Processors

It is assessed that the GP practice is acting as a Data Controller since they define the purpose and manner for processing of the patient data held within the health record.

It is asserted that MMS® are a Data Processor. This is because they will be acting on the narrow instructions of the GP practice with regards to what data they access, collect and

amend. The judgements that they are making do not demonstrate a sufficient level of autonomy that would define them as a Controller, rather, they are using nationally available guidelines to make recommendations to the practice about how medication might be optimised for the patients. The Practice will define the scope of service and identify particular patient cohorts.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that the Controller and Processor relationship has not been sufficiently defined and documented. This may result in ineffective management of risk and could result in improper management of data subjects' personal data.	Low	Low	Low	Controller and Processor relationships defined within DPIA	Eliminated	Low	DPO Approved Aug 20
There is a risk that the Processor is not engaged by virtue of an Art 28 compliant processing contract. This could result in the Processor managing data subjects' personal data improperly.	Moderate	Moderate	Moderate	MMS® has been provided with a template processing contract that complies with Art 28 Confirmed that data will not be used for research and no data will be printed.	Reduced	Low	DPO Approved Aug 20

3. Lawful Processing

This assessment confirms the following with respect to the lawful processing of personal data;

- The information being processed constitutes personal and special categories of personal data
- The data being processed is necessary for a public task; Art 6 (1) (e)
- The data being processed is necessary for medicine; Art 9 (2) (h)
- Common law confidentiality is satisfied since the Controller has merely delegated their Controller functions to a third party. Privacy notices make it clear that such disclosures will happen when they state that data will be used for “Undertaking clinical audits locally to ensure safety and efficiency”.

KAFICO


INFORMATION · GOVERNANCE · CONSULTANCY

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that patients do not reasonably expect the involvement of a third party in this way and that they might regard such a disclosure as unauthorised.	Low	Moderate	Low	Privacy materials have indicated that these types of activities happen for some time and so the feeling is that there is a general expectation among the patient population. Any direct contact should make it clear that they associated with the practice.	Reduced	Low	DPO Approved Aug 20

4. Minimisation and Retention of Personal Data

Data protection law provides that Controllers must not keep personal data for longer than it is needed and that you should create a policy, setting standard retention periods wherever possible, to comply with documentation requirements. Additionally, only the minimum data necessary for perform the identified tasks should be processed.

The following fields will be accessible to MMS® during the project and a rationale has been provided for each.

Title	Use / rationale
Name	Identifies patient such that it is possible to make individual recommendations for therapy
DOB	As above used to verify identity if communicating with or about the patient
NHS No	Mandatory national identifier
Address	As above used to verify identity if communicating with or about the patient
Postcode	As above used to verify identity if communicating with or about the patient
Sexual Health	Available due to the inability to limit the view within 
Ethnic Origin	May have considerations impacting recommendations for medications
GP Name	Required if it is necessary to contact GP regarding recommendations
Gender	May have implications on medication doses

KAFICO

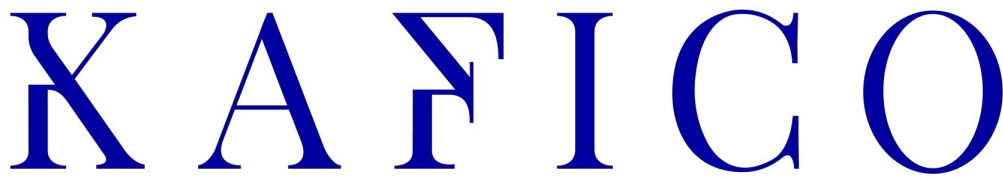
INFORMATION · GOVERNANCE · CONSULTANCY

Next of Kin	Available due to the inability to limit the view within S1
Diagnosis	Relevant to review medication appropriately
Consultant Name	Available due to the inability to limit the view within S1
Medical History	Relevant to review medication appropriately
Treatment Information	Relevant to review medication appropriately

The assessment concludes that there appears to be a suitable rationale for all data fields collected during the questionnaire. Whilst there are a few fields that are available to the Processor due to technical limitations of the system, it is considered that the full audit trail offered by Smartcard access supports minimisation of access as much as possible.

With regards to retention periods, the Processor will access the clinical system directly, using allocated SmartCard access via a secure VPN connection and so there will be no data downloaded or created within MMS® systems or physical assets as part of the project. Data will remain within the practice clinical system and be retained in accordance with existing retention schedules.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that the MMS® are able to access data fields that are not necessary or relevant to the project at hand. This may result in an unauthorised access and a risk to the rights and freedoms of the data subjects.	Moderate	Low	Moderate	Data processing contract must make it clear that only data fields relevant to the project must be accessed. Practice should undertake access audits to ensure appropriate access during and following the project.	Pending	Pending	DPO Approved Aug 20



— INFORMATION · GOVERNANCE · CONSULTANCY —

5. Fair and Transparent

GDPR Article 12 provides that data subjects must be provided with particular information in order for processing to remain lawful. The below assessment is undertaken on the standard practice materials provided by Kafico. Where practices have other materials in place, there is a need to make independent assessments.

The grid below identifies whether the components of informed consent are present.

Requirement	Website materials and poster on site	Status
Individuals are informed of the types of personal data collected	Under “Your Information”	Present
Informs individual of the purposes for which Personal Data is collected and used	Under “Your Information”	Present
Informs individual of how to contact the organization with any inquiries or complaints	Under “Information Rights”	Present
Individuals are informed of type or identity of third parties to which it discloses personal information and the purposes for which it does so	Under “What We do with Your Information” - <i>Discuss or share information about your health or care with other health or social care providers</i> Under “What else do we do with your information” - <i>Undertaking clinical audits locally to ensure safety and efficiency</i> Under “List of Providers”	Present
Individuals are informed of their choices and the means available for limiting the use and disclosure of their Personal Data	Under “Information Rights”	Present

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Individuals are informed about the Independent dispute-resolution body designated to address complaints free of charge	Under “Information Rights”	Present
Individuals are informed about the requirement to disclose EU Personal Data in response to lawful requests by public authorities	Under “Sharing When Required by Law”	Present
In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 or Article 9 must be specified.	Under “Your Information”	Present
<p>[notices must include] how the data subject can take steps to exercise [rights] to;</p> <p>access;</p> <ul style="list-style-type: none">· rectification;· erasure;· restriction on processing;· objection to processing <p>and</p> <ul style="list-style-type: none">· portability. <p>withdraw consent (easy as to give consent)</p> <p>In particular, the right to object to processing must be explicitly brought to the data subject’s attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information</p>	Under “Information Rights”	Present

Since the standard practice notice contains the necessary elements of Article 12, it is determined that the fairness and transparency requirements of data protection law are maintained.

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that data subjects are not made aware of the existence of MMS® as a processor or that medication reviews are undertaken in this way. This could result in a risk to the rights and freedoms of individuals.	Moderate	Moderate	Moderate	MMS® should be added as a processor on the practice transparency materials. A 'news ticker' notice should flag the medication review process.	Pending	Pending	DPO Approved Aug 20

6. Information Rights

The assessment confirms the below position with respect to information rights

Right to Access	The data processed by MMS® will be added to the clinical record and so will be available through the usual access routes
Right to Rectification / Restriction	altered by the project
Right to Erasure	Not altered by the project
Right to Portability	Not altered by the project
Right to Object	Not altered by the project

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that patients will not be aware of changes being made to their clinical record and therefore will not have the opportunity to engage their right to rectification or being informed.	Low	Moderate	Low	Patients shall be included in any changes to their medical record resulting from the review.	Pending	Pending	

7. Accuracy and Data Quality

There are a number of measures employed to promote data quality by MMS®. The MMS® Confidentiality Policy provides that MMS® will;

- Conduct routine audits of [their] information assets in line with MMS® Information Governance Policy
- Ensure Data users record information accurately and take reasonable steps to check the accuracy of information they receive from data subjects or anyone, regularly checking all systems to destroy out-of-date information and correcting inaccurate information.
- The retention policy in place also provides that “ensure data quality all staff must observe confidentiality & integrity of information stored and processed. Information is only useable if it is accurate, correctly and legibly recorded, kept up to date and easily accessible when needed.”.

MMS® will be accessing existing data sets and making corrections and amendments based on current best practice and so data quality and integrity is at the core of the project.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that changes made within the system by MMS® will not have proper oversight by the Controller and this may result in the data subject not being fully aware or confusion around how particular changes or additions came about.	Low	Moderate	Low	Smartcard access is fully auditable and provides an audit trail of any changes made to data subject records. MMS® will produce a final report of any changes and amendments made to the system.	Pending	Pending	

8. Technical and Organisational Measures to Protect Personal Data

The processing performed by MMS® is one that is usually carried out through physical presence at the practice site. The current pandemic has meant that many services are now delivered remotely. However, there is still a need to ensure that services are suitable for remote

KAFICO

— INFORMATION · GOVERNANCE · CONSULTANCY —

delivery and that technical and organisational measures in place provide robust protection for the rights and freedoms of individuals.

Due to the nature of the information being processed and the inherent vulnerabilities of some of the patients included, it is reasonable to conclude that that access to patient records by an external third party represents at least a moderate to high degree of risk to the rights and freedoms of data subjects in the event that appropriate technical and organisational measures are not put in place at all.

This assessment will therefore explore each of the elements drawn out within data protection legislation and guidelines for mitigation of those risks such that the risk is at an acceptable level.

Security of Data Hosting

The data accessed by MMS® for the project will remain within the clinical system of the Controller. Access will be granted via Smartcard which will be used on laptops which are connected via the HSCN.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that data will not be secure in transit / during direct access by MMS®. NHSD provide that "Whilst these capabilities undoubtedly enhance network security, Like N3 previously, HSCN should not be considered a 'secure' network. All connected organisations must risk assess their use of the HSCN and employ their own security controls"	Moderate	High	Moderate	As proposed, MMS® use the additional security of a virtual private network in conjunction with HSCN connection, given the nature of the information and vulnerability of data subjects.	Pending	Pending	DPO Approved Aug 20

Security of Data in Transit

The data accessed by MMS® for the project will remain within the clinical system of the Controller. Access will be granted via Smartcard which will be used on laptops which are connected via the HSCN. See risk identified above.

Pharmacists will also have access to NHS Mail which will allow communication with practice team members during the service delivery. NHS Digital provide that "NHSmail is accredited to

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

government OFFICIAL status for sharing patient identifiable and sensitive information, meaning it meets a set of information security controls that offer an appropriate level of protection against loss or inappropriate access.”

It is therefore assessed and concluded that data has been effectively secured in transit.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that MMS® will use NHSMail to communicate with non NHSMail users such as patients. End to end encryption will therefore not be assured and this could result in a risk of interception and a breach of confidentiality.	Low	Moderate	Low	MMS® confirm to the Controller that they will not use NHSMail to contact any non NHSMail users.	Pending	Pending	
There is a risk that MMS® may telephone patients directly and disclose information inappropriately or in a way that does not comply with practice policy.	Low	Moderate	Low	Controller to confirm to MMS® their policy on leaving voicemails for patients and confirm how they must identify themselves to patients.	Pending	Pending	

Continuity and Availability

MMS® have confirmed that they have a Business Continuity Policy in place and the service being delivered is supplementary. It is therefore assessed that this service would likely not be considered business critical. Were there failures around connectivity or access, the Controllers have existing manual processes available and therefore it is assessed that the technical and organisational measures to ensure the availability of data are sufficient.

Access Control

MMS® will be granted direct access to the clinical system by virtue of Smartcards. NHS Digital provide that “A smartcard used in conjunction with a passcode, known only to the smartcard holder, gives secure and auditable access to national and local Spine enabled health record systems”.

The data is not stored on local systems and any access, additions or amendments made are fully auditable by the Controller.

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of	Inherent Severity of	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure active and approved
There is a risk that MMS® will be granted an inappropriate level of access to the system resulting in a risk to the rights and freedoms of data subjects and a breach of the minimisation principle.	Low	Moderate	Low	Controller must ensure that Smartcard access granted is appropriate for the service being delivered and based on the principle of 'least privilege'.	Pending	Pending	DPO Approved Aug 20
There is a risk of unauthorised access to patient records such that is inherent with any access to systems containing personal data. This could result in a risk to the rights and freedoms of individuals.	Low	Moderate	Low	Controller must undertake a random audit during the duration of the project to ensure that access aligns with the scope of the project and services.	Pending	Pending	DPO Approved Aug 20

Pseudonymisation and Encryption of Personal Data in Transit and at Rest

Data is required in identified form to support the delivery of the identified purposes.

Policy, Training and Confidentiality

MMS® have provided copies of their Confidentiality, Information Governance, Incident Management and Records Management Policies. They have also confirmed that all staff members are trained regularly in information governance.

The Processor has confirmed that checks have been made against the following;

- Pharmacist registration / practicing details
- Smartcard details
- DBS
- Professional insurance

It is therefore concluded that the given the nature and volume of personal and special category data being processed for this project, there are technical and organisational measure in place such that the inherent risk is reduced to an acceptable level. If the identified mitigations are put in place, it is considered that there are no residual issues that result in a high risk to the rights and freedoms of individuals.

KAFICO

— INFORMATION · GOVERNANCE · CONSULTANCY —

Controller has checked that MMS® have submitted an NHS Data Protection and Security Toolkit for 2020.

9. Sign Off

Item	Name / Position / Date	Notes
Measures approved by:	Emma Cooper, Kafico Ltd, August 2020	It is concluded that the stakeholders have in place appropriate technical and organisational measures to protect personal data and have identified no residual risks that would be considered high and require escalation to the ICO.
Residual risks approved by:	Emma Cooper, Kafico Ltd, August 2020	
Data Protection Advice provided:	Emma Cooper, Kafico Ltd, April 2020	Mitigations identified should be confirmed by both Controller and Processor.
Periodic DPIA review dates:	Emma Cooper, Kafico Ltd, August 2020	October 2020 Review Due