DPIA – EMIS Web

Submitting controller details

Name of controller	The relevant customer
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

EMIS Web is a clinical system for delivering integrated healthcare. EMIS Web allows healthcare professionals to record, share, and use vital information, so they can provide better, care that is more efficient. EMIS Web allows primary, secondary and community healthcare practitioners to view and contribute to a patient's electronic healthcare record.

EMIS Web has been designed to improve efficiencies and maximize patient safety. Inbuilt templates and protocols make daily tasks easier, and sophisticated clinical decision support operating in real time empowers healthcare teams to provide the best possible care to patients. Comprehensive search and reporting functionality, enabling users to harness the power of their data to review performance, manage audits and evaluate population health, from local to enterprise level.

EMIS Web is connected to many services; large parts of the NHS send and receive data with EMIS Web, or through connected services such as PFS, Partner APIs, EMIS Web Mobile, GP Connect, Mesh, and the NHS SPINE.

EMIS web is software solution for primary care organisations, containing and sharing personal and sensitive data. This data is encrypted in transit. The Data Controllers for EMIS Web are GP organisations, and Data Recipients are set up by the data controller as per sharing agreements. EMIS acts as a Data Processor.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

- GP Practice joins EMIS and migration team moves their data from current system to EMIS Web format through the standard Migrations process.
- A Clinical User (controlled locally by admins at the setting) pulls up a patient record and is able to either view or makes changes based on local RBAC controls.
- If the user is at a spine activated site and signed in with smart card, if demographics, prescription, transfers to practice or electronic referral changes are made (to a record where a patient is opted into SCR) this change is written from EMIS Web to the NHS Spine. Some practices are not enabled so this does not go to spine. If possible, the record pulled up is compared to spine, and if there are differences, the user can reconcile differences, change the record and then when they save changes, this goes to the spine, which pushes the data out to where it needs to be.
- In England, Web auto files results and some other data that come to EMIS Web. Auto filing is a notification task where a clinician will have awareness of auto filing happening but no actual user interaction is required. This workflow is not for all inbound data- specifically Covid- NHS England decided no need for anyone to have to deal with them, but e.g. lab results come into inbox area as a task for GP to look at results, so they should take action based on those and would follow a different workflow. Different types of tasks based on different systems.
- GP connect can book appointments through- shows these in appointment system. This is the same with integration partners. Partners can file into EMIS web without message or task, with no user interaction needed.
- Records are persisted, but retention periods will apply to certain data as per NHS standards.
- Differentials are daily and weekly backups and yearly backups. Yearly back-ups are kept forever, monthly are cycled every 12 months and Daily and weekly are cycled more frequently. NetBackup store data in an encrypted tape in a secure third party premises.
- EMIS Web data is in multiple privately run datacenters places for Business Continuity

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Personal Details:

Name

Date of birth/death

Contact Details:

Address

Postcode

Telephone number

Personal email address

Work email address

National Identifiers:

NHS number

Passport number

National Insurance number

Other Contacts:

Next of Kin / ICE

Guardian/Carer Details

System Identifiers / Tracking:

Online identifier

Location data (GPS, IP, MAC) (for users/clinicians)

Health Record Types:

Full Medical Record

Partial Medical Record

Prescriptions

Testing Results

Clinical Studies

Vaccination Information

Special Category Data:

Information relating to sex life or sexual orientation

Genetic data

Race

Ethnic origin

Religion

Free text fields could contain additional information. This additional data could be recorded for Alerts, e.g. patient can be violent and could mention convictions. EMIS do not control this free text field, and clinicians should take care to ensure that this is appropriate.

The data processing is somewhat configurable by the GP, but it is understood that all access should be appropriate and give minimal data based on the Caldicott principles. All EMIS Web access is RBAC controlled locally. The data processed is to enable identification of the patient and to receive appropriate care.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Data Controller: GP's / Clinical Organizations

Data Processor: EMIS / Potentially other third parties integrated into EMIS Web or clinical settings

Data Subjects: Patients / Practice Contacts / Clinicians

Data Recipients: GP Practices / Clinical Organizations / CCMH and Community (any clinical care setting that purchases EMIS Web) (Pharmacies and acute care settings can view shared GP records in ProScript Connect by Requesting from EMIS Web. This depends on agreements being in place prior to access being provided).

Data sets processed as part of this project may contain; Personal Details, Contact Details, National Identifiers, Other Contacts, System Identifiers / Tracking, Health Record Types, and Special Category Data for both legal adults and minors. Patient consent is the GP Practices or healthcare provider's responsibility; EMIS can have a view of patient consent options entered by the user that Record NDOP and other relevant opt out codes. There may also be scope for EMIS to view subsections for granular consent for part of research cohorts, as agreed with data controllers via Data Sharing Agreements.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Data in the cloud is key encrypted. Access control policies (RBAC) are managed locally by practices on private networks. Where there is no encryption, there is a Layer of networking- firewalls etc.

Access is all immutably audited. All scripts are recorded as part of the audit log.

The end user audit log can be accessed through EMIS Web and is immutable. All support access also shows in this audit trail.

Some specific end users for EMIS Web have local servers in the practice that data can be replicated onto. All medical data in these is encrypted, aside from the patient demographics. Demographics are not encrypted because users have to search on Demographics and if these had to be de-encrypted while searching the latency would hugely increase.

In local servers, there is a cache type storage based on appointment books etc. This means practices can pull data locally for better performance if there are issues elsewhere on the server. Also this forms a BC system so if users lose connection, there is read only copy of data that can be accessed. This data records appointment books, demographics and SCR for patients booked in and why they have come in (reason for appointment if available).

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Whom else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Relevant stakeholders are involved throughout the assurance processes, which may include Information Governance, Information Security, Clinical Safety, Legal and Contracts, Product and Development, and other relevant teams. EMIS is accredited with ISO 27001:2013 Information Security; ISO 9001:2015 Quality; Cyber Essentials Plus; ISO 20000:2018 Service Management; ISO 22301:2012 Business Continuity; ISO 14001:2015 Environmental Management - LC15 and is registered with the ICO Z2670786.

Additionally, EMIS Group has a Standards Exceeded DSPT.

EMIS Group Security team consists of the Chief Information Security Officer (CISO also SIRO), Security Management, Security Architects and the Information Governance team. The team's responsibility is to ensure good security practice across the group, whether that is technical security, data protection, Information governance, business continuity or security management expertise. EMIS Group review Information Security policies annually or when any significant changes. Senior Management approves these.

EMIS Web undergoes penetration testing on an annual basis, and whenever there are new updates or changes to the system to ensure system security of a high standard. Security for the solution in a live environment will be the responsibility of both EMIS and the users of the software; users will be expected to maintain standard security of physical machines using EMIS Web.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Legal bases for processing are covered under consent, contract, and legal obligation.

Coroner’s requests could be covered by Legal obligation. Additionally, any disciplinary or court requests would be covered by legal obligation.

EMIS have contracts with all of our customers and partners interacting with EMIS Web, alongside relevant data sharing agreements.

Patients and controllers consent to processing, either explicitly or via implied means.

EMIS have legitimate interests to process this data as a key service provided by our business.

Processing related to EMIS Web is all very well justified. The data subject consents to this data being processed when they join the participating EMIS Web Practice, and they have the option to opt out of processing where applicable. All processing is for health and social care provision (and sometimes for public health or legal obligations); contracts between EMIS and our Partners and customers cover all processing. Various DSAs are in place at the customers discretion where required for any processing involving third parties. EMIS only processes the data according to the contracts and DSAs in place with the customer.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Loss of Data	Remote	Severe	Medium
Inappropriate processing of Personal Data	Remote	Moderate	Low
Inappropriate Data Transfer	Remote	Severe	Medium
Excessive Data Processing	Remote	Moderate	Low
Data Integrity	Remote	Severe	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Loss of Data	Regular backups of data, (Yearly, monthly, and daily where necessary).	Reduced	Medium	Yes
Inappropriate processing of Personal Data	Role Based Access Controls, managed by end users.	Reduced	Low	Yes
	Secure methods of data transfer, such as SFTP,	Reduced	Medium	Yes

Inappropriate Data Transfer Excessive Data Processing Data Integrity	MESH, NHS Spine, etc.; additionally, data encryption during transit and at rest. All data processed is essential to purpose, however is significant. Patient consent is captured to process data. Responsibility of the data controller.	Reduced Reduced	Low Medium	Yes Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
DPIA Approved by:	Courtney Lee-Hentze Information Governance Analyst	
This DPIA will kept under review by:	IG team	The DPO should also review ongoing compliance with DPIA