Medstars Data Protection Impact Assessment

Submitting controller details

Name of controller	Joey Islam
Subject/title of DPO	Director
Name of controller contact /DPO (delete as appropriate)	Joey@medstars.co.uk

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.

Need for a DPIA

Medstars Connect is an innovative health communications solution based upon the latest scalable, configurable mobile app technology. It has been designed by senior NHS clinicians familiar with NHS infrastructure and requirements. Our founders are medical consultants of 10 years standing in Birmingham, specialising in mental health, pre-operative medicine, anaesthesia and surgical delivery.

The platform is focused around scheduled video and live chat consultations, file/photo sharing, shareable post-appointment notes and secure messaging. The app is designed to be intuitive, hassle free and anyone who has used a mobile phone will be comfortable using it. It includes browser-based appointment scheduling software, enabling administrative staff to manage clinics on behalf of clinical staff, maximising clinic efficiency. There is also a flexible browser-based video consultation alternative for clinicians who prefer to use existing Trust hardware for remote consultations.

Need for a DPIA

Medstars processes special categories of data such as individuals' Personal Identifying Information (PII), i.e. name, age, address and healthcare data.

The need for a DPIA is the processing on a large scale of special categories of data for the use of the Medstars platform to:

- Issue SMS messages to patients' mobiles.
- Exchange and store emails, images/documents/files and chat messages between patients and clinicians.
- Enable video consultations (which can be recorded or stored as required by the data controller) between clinicians and their patients.

Further detail can be found here, www.medstars.co.uk/documents

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.

Data Processing

How will you collect, use, store and delete data? PII data is collected and consent gained through the registration process for an individual patient. Clinician email address and professional regulatory body number are provided by the commissioning organisation, this 'white' list is used to validate registrations by clinicians.

Healthcare data is exchanged during a consultation between the patient and clinician. The video consultation service is hosted by Vonage who are fully compliant with GDPR. The video and audio communication is only visible to participants on the call and is only recorded or stored on specified UK servers if commissioned by the NHS organisation and consent is gained from the patient by the clinician.

All data is stored on UK based servers under AES256 encryption and managed according to our Records Management Policy, this details ownership, document retention protocol and other requirements.

What is the source of the data? PII data is gained by explicit consent of the patient. Clinical data is gathered from both the clinician and patient during the consultation.

Will you be sharing data with anyone? Medstars Ltd will only share data with those parties we have a contractual relationship for data processing with and private individuals exercising their right to access personal data pertaining to them.

What types of processing identified as likely high risk are involved? Sensitive data or data of a highly personal nature.

What is the nature of the data, and does it include special category or criminal offence data? It includes personal data but not criminal offence data.

How much data will you be collecting and using? As Medstars is a new company we have no history of volume use to inform this question. However, volumes will be dependent upon the size of the contract with either the NHS or other organisations. We will update this statement following further trading experience.

How often? Data will be collected and used on a daily basis once contracted.

How long will you keep it? As per The Records Management Code of Practice for Health and Social Care 2016.

How many individuals are affected? Dependent on contract.

What geographical area does it cover? Typically the UK, but this will depend upon the specific contract.

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.

What is the nature of your relationship with the individuals? We are a consumer supplier of services to the NHS and other healthcare organisations.

How much control will they have? Individuals will be able to exercise their data 'opt out' rights, they have the right to request that we stop processing personal data for our legitimate interests and withdrawal of their consent.

As required by the Regulation, consent is easy to withdraw, Data subjects may request that Medstars does not process your personal data, at any time. Data subjects may contact us to withdraw your consent using the contact details on our website.

https://medstars.co.uk

Would they expect you to use their data in this way? Yes as explained prior to obtaining consent.

Do they include children or other vulnerable groups? Yes.

Are there prior concerns over this type of processing or security flaws? None identified.

Is it novel in any way? No.

What is the current state of technology in this area? All of our software is the latest technology and meets current data protection requirements.

Are there any current issues of public concern that you should factor in? None identified.

Medstars has Cyber Essential Certification registration number IASME-A-08250.

What do you want to achieve? The purpose of data processing is for the invitation, scheduling and enabling of remote video consultation services between clinicians and patients.

Consultation process

As part of our tendering process, all relevant GDPR documentation will be provided to the prospective data owner for their review and approval.

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.

Necessity and proportionality of data processing

What is your lawful basis for processing? Medstars processes personal data as set out in the guidance given in Article 6 of the GDPR. The following items are relevant:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (Article 6 (1) (a) (Consent)
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (Article 6 (1) (f) (Legitimate Interest).

Does the processing actually achieve your purpose? Yes.

Is there another way to achieve the same outcome? No.

How will you prevent function creep? We have designed and implemented controls, both in the system design and business practices, that can limit function creep? Privacy is protected by the implementation of privacy safeguards directly into the core architecture of our product, so that it would be difficult to intrude on privacy if used by others. Medstars manages any system development through its comprehensive project management framework and robust governance processes to prevent misuse or cross use of data sets.

How will you ensure data quality and data minimisation? This is covered in our Data Quality policy. The availability of accurate and timely data is vital for the safety of the people we care for and the safe and responsible running of our organisation. This policy outlines the following procedures for ensuring data accuracy, minimizing the uses of data, correction of errors.

What information will you give individuals and how will you help to support their rights? Individuals have the right to request that we stop processing personal data for our legitimate interests and withdrawal of their consent.

As required by Regulation, consent is easy to withdraw, Data subjects may request that Medstars does not process their personal data, at any time. They may contact Medstars to withdraw your consent using the contact details on the website, https://medstars.co.uk. There is also the option to withdraw consent at any time.

What measures do you take to ensure processors comply? Applying appropriate due diligence involving audit reviews, spot checks, policy for breaches and escalation.

How do you safeguard any international transfers? We do not undertake international transfers, the entire platform is hosted on UK servers. All data are securely encrypted, whilst in transit and at rest. *NB, in the event of a consultation occurring when a clinician or patient is outside of the UK, data may be processed on the clinicians computer and a patient may receive a text through a non UK network.*

Risk assessment

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.

Malicious risks Attempts by malicious actors to intentionally breach security.	Low	High	Low
Fraud Deliberate misuse or sabotage of systems, data by employees.	Low	High	Low
Negligence risks Inappropriate and unintentional sharing of personal data by clinicians.	Low	High	Low
Process risks Failure to update and / or apply relevant data security and protection policies (e.g. anti – virus) to infrastructure (PC's, phones). **NB.** Events such as abusive communications between individuals are outside of scope.	Low	High	Low

Risk Mitigation

Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no
Malicious risks Attempts by malicious actors to intentionally breach security.	Accredited Cyber security, latest security protocols, application of data security and protection policies.	Reduced	Low	Yes
Fraud Deliberate misuse or sabotage of systems, data by employees.	Application of data security and protection policies. This will include for example, password complexity and encryption. The consultation process requires mutual identification. Full audit trails are captured.	Reduced	Low	Yes
Negligence risks Inappropriate and unintentional sharing of personal data by clinicians.	Patient and clinician email addresses are withheld from the patient. A clinician must use at least of two pieces of PII to validate	Reduced	Low	Yes

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.

	patient identity before a consultation can be scheduled. A further validation step is undertaken by the clinician at the beginning of the video consultation. The system displays two pieces of PII allowing the clinician to validate identity. The patient is also shown the clinicians name and photograph allowing them to confirm identity. Assigned owner for data security and protection. Staff training and awareness of relevant policies. Audits and spot checks.			
Process risks Failure to update and / or apply relevant data security and protection policies (e.g. anti – virus) to infrastructure (PC's, phones).	Application of data quality and maintenance policy by both data owners and processors.	Reduced	Low	Yes

Sign off and outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	Joey Islam Director 06.05.21	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Paul Moran NHS Programme Lead 06.05.21	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Joey Islam Director 06.05.21	DPO should advise on compliance, step 6 measures and whether processing can proceed

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.

Summary of DPO advice: Processing can proceed.		
DPO advice accepted or overruled by:	Mahnaz Hashmi Co-founder 07.05.21	If overruled, you must explain your reasons
Comments: Approved.		
Consultation responses reviewed by:	Barry Lambert Co-founder 07.05.21	If your decision departs from individuals' views, you must explain your reasons
Comments: Approved.		
This DPIA will kept under review by:	Paul Moran NHS Programme Lead 07.05.21	The DPO should also review ongoing compliance with DPIA

Please note: Medstars is a data processor and when using our platform, it is your organisation's responsibility to complete a DPIA. This document will help inform your inputs.