****

**Data Protection Impact Assessment – Clinic.co**

***As the data controller, when using Clinic.co, it is up to clinicians and their organisations to complete a DPIA. To support this, we have put together this document to address key elements of DPIAs for our partners.***

At Clinic.co we handle sensitive patient data and take our responsibilities under GDPR very seriously. In this DPIA, we set out how we comply with GDPR to provide clinicians and end users with assurance that your data is safely managed. Overview:

* **Secure Video Consultation:** Clinic.co is fully secure and compliant with GDPR, ISO27001, ISO9001 and DCB0129. Video and audio communication is only visible to participants on the call and transmitted over an encrypted connection. It is not recorded or stored on any server unless initiated by the clinician. When recorded, it is safety stored in servers based in the UK.
* **Secure Data Processing**: We host our servers in the UK (via Amazon Web Servers). We are Cyber Essential compliant and our technology stack and systems are compliant with the NHS Data and Security Information Toolkit.

**1.Scope**

Organisations use of Clinic.co. Clinic.co is a technology platforms designed for clinical triage and telemedicine. Clinicians sends a text or email to the patient, containing a link. When pressed on, the patient is prompted to provide consent to share video. Upon consent a video stream is established which enables stream to the clinician. Clinicians can live stream or store video. Clinician can share stream or recording via text/email.

A DPIA is required as large scale sensitive patient identifiable information (i.e. images streamed from a smartphone or other device) is being processed and transmitted. Data includes:

* Clinician staff data (typically name, role, organisation, contact details)
* Patient data (typically name, identifiers, contact details - mobile number and email)
* The video and audio communication of any video consultation is only visible to participants on the call, and is not recorded or stored on any server unless initiated by the clinician.
* Clinicians can also share their screens to show patients images or share medical information with them. This is not recorded or stored on any server unless initiated by the clinician.
* For our premium service, where patients are self paying, we offer clinicians the ability to bill patients directly using vetted sub processors to manage payments.

**2. Nature of processing and benefits**

The source of the data will be a patients smartphone, computer or tablet where they have agreed to allow the use of its camera via a secure video-link. The video-data captured will only be available to the clinician of the organisation, although the products of that data can be used to inform clinical assessments which may then be shared with others involved in the individual’s direct care.

No particularly high-risk data processing is involved as compared to conventional hear-and-treat and see-and-treat processes. It is the case that there will be more video data accessed than previously. Video will capture special category health data. However, for clinicians, it effectively supplies comprehensive information along existing data flows, rather than ‘new’ data flows.

The nature of the data is a live video stream (plus audio from the call) of a patient/their injuries or condition/the circumstances in which they are contacting the clinician. This approach to communication should only be used if the patient wishes to use the system and actively takes steps to activate the video-link. If a patient does not want to use video consultation, then data will not be captured.

There are times where the call handler / clinician may not correctly assess the patient as they are doing so based on what the caller is telling them. There will be occasions where a patient cannot or does not fully / accurately explain their condition. A live video stream provides a clear picture to the clinic an – enabling them to see and treat, rather than hear and treat.

Key benefits:

* Clinician can make more accurate assessments and treat patients remotely.
* Supports clinicians to be more efficient in dealing with the increasing number of calls and determine appropriate pathway.
* This improves clinician safety – i.e. coronavirus and other patients in practice.
* Improves patient access to a clinician – works on any device with no software download required.

**3. Type of processing**

* Special category - video data.
* Basic identifier - Mobile phone number/email address.
* Medical records where the clinician shares screen with patients

**4. Consent**

* All callers are given the option of using the clinic.co system and asked to actively click on the hyperlink to confirm consent to provide with live streaming.
* The message from the caller can be amended by the clinician if specific consent is required

**5. Data storage**

There are three options for video storage: Not stored, stored in AWS (GDPR, NHS approved) cloud, or stored locally via an API that pulls the video to clinicians own server. For our basic service, no video is recorded. Clinicians have the option to store video if using our premium service. In these scenarios, recordings are fully auditable and the retention period can be determined by the clinician. No data is stored on the patients device.

**6. Data Security**

* System uses AES 256 Encryption.
* To use the system, clinicians need to authenticate accounts. Clinic.co and GoodSAM hold ISO 27001 and ISO9001.
* HIPPA and GDPR compliant.
* Meets DCB0129 standard.
* We are Cyber Essentials certified.
* Compliant with the NHS Data and Security Information Toolkit
* Clinic.co uses SSL / TLS 1.2
* All our services adhering to WCAG2.1 Guidelines for accessibility

**7. Necessity and proportionality**

The lawful basis for processing is Article 6(1)(e) GDPR and Article 9(2)(h) GDPR, read with Schedule 1 paragraph 2 of the Data Protection Act 2018.

Clinic.co provides an effective solution to improve care. Other solutions (non-video) would not provide comparable quality of information to assess / treat patients. In the context, achieving the same outcome through non-video means is not possible.

Clinic.co provides flexibility to clinicians in terms of proportionality of data collection – video can be stored (in-house or with clinic.co) or live streamed.

**8. Data minimisation**

Data minimisation will occur because clinic.co does not, as standard, retain footage from the video consultations. Video consultations can be deleted directly from th system when required.

**9. Cross border data flows**

The Clinic.co AWS Server is in the UK and so video (data) will not leave the UK.

**10. Review of GDPR Risks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source of Risk**  | **Control Measure**  | **Likelihood of harm** | **Severity of Harm** | **Overall Risk** |
| The filming may lead to sensitive images (e.g. of an individual in pain/of injuries) being obtained, which is intrusive to the patient’s privacy.  | Used in controlled clinical environment (restricted area and only staffed by individuals who owe contractual and/or professional obligations of confidence) | Low | Low | Low |
| Data is leaked through the provider of the service. | Data sharing agreement available, arrangements to control access to video footage/dashboard.Clinic.co undertakes regular penetration testing. Audit of videos viewed (and identity of viewer) available. No third parties providers used – all software coded in house.  | Possible | Severe | Low |
| Data is leaked by clinician/user/call handler | Individual log ons to segment clinician access. Audit of videos viewed (and identity of viewer) available. | Possible | Severe | Low |
| Patient does not consent from use | In order to enable video stream, patients needs confirm consent | Low | Severe  | Low  |
| Inadvertent collection of data  | Data stream terminated both ways – by clinician (ending call) or caller (closing hyperlink). Once stream terminated, it cannot be re-established. No data stored on hardware/device.  | Low | Severe | Low |

**11. ICO Registration Information**

Registration number of Clinic.co Ltd: ZA201864

Date of first registration: 25 August 2016

For any questions relating to information governance, please contact Clinic.co: info@clinic.co and we would be happy to assist you.