Pando

Data Protection Impact Assessment

Introduction: This document details the data protection impact assessment (DPIA) carried out by Forward Clinical Ltd with regard to the use of Pando as a mobile application at any given NHS trust, hospital or other organisation.

Purpose: The purpose of a data protection impact assessment is to identify any new collection or uses of potentially sensitive data, to assess the possible risks associated with these and to allow organisations to make an informed decision about the technologies they employ with regards to data collection, use, or sharing.

Scope: This data protection impact assessment relates to the use of Pando as a mobile application within a clinical setting. It refers to the current data protection laws as they stand, although it will continue to be reviewed regularly to take into consideration ongoing regulatory change. Forward Clinical Ltd reserves the right to update this data protection impact assessment as necessary, particularly with regard to the changing landscape of data protection law.

Background: It is necessary to complete at DPIA whenever a significant change is made to the way in which data is collected or processed by an organisation, to ensure that the impact of this on the data subject and their rights has been fully considered.

As described by the ICO, the steps involved in completed a data protection impact assessment are:

1. Identify the need for a DPIA.
2. Describe the processing/information flow.
3. Consultation process.
4. Assess necessity and proportionality.
5. Identify and assess risks.
6. Identify measures to reduce risks.

Table of Contents

Data Protection Impact Assessment (DPIA)

Data protection impact assessment screening questions

These questions are intended to help decide whether this DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise.

Question	Answer *Please add any relevant comments*
Will the project involve the collection of new information about individuals?	No
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	No
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	Yes – encrypted transfer and secure storage (encryption of data when at rest and access authentication) of private health records. There is a universal privacy expectation that highest levels of information security will be deployed.
Will the project require you to contact individuals in ways that they may find intrusive?	No

Step 1: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

Pando is a smartphone application and communication tool for clinical teams. Pando has been purpose-built for medical staff and is designed to support high-quality, secure and compliant instant messaging for individuals or groups. Available for both iOS and Android, the app has a few simple key features:

- Secure, compliant instant messaging, including sharing of photos
- Live task management and workflow tracking
- Sharable patient profiles & patient lists
- Hospital directory function.

Forward Clinical Ltd is motivated by a desire to save time wasted on the inefficient, archaic communication methods used by many in the NHS. Modern NHS hospital care is fast-paced and increasingly complex as clinical teams deal with a higher volume and turnover of patients whose care typically involves multiple tests and interventions. As a result, teams must collaborate ever more closely to deliver high quality care. This is currently difficult to achieve since hospital communication systems rely on technology from the 1970s such as pagers, telephone switchboard and printed lists of patients; our belief as clinicians ourselves, and from survey data collected from over 120 doctors, is that these tools are not fit for purpose in the modern NHS. Busy NHS clinicians are rarely desk-bound with immediate access to a desktop PC or laptop whilst delivering, managing or planning patient care.

Public email platforms such as Google Mail, Office 365 and NHS Mail (limited functionality by only providing secure messaging) have either been deemed unsuitable due to limited functionality or non-compliance with NHS Digital data security policies, NHS IG Toolkit Guidelines and the Data Protection Act.

Pando additionally provides a Trust with high-levels of technical data security assurance such as high levels of encryption in transit and at rest (minimum AES 256-bit standard for data encryption in-transit and at-rest). In transit data is encrypted and transferred via HTTPS (TLS v 1.2 min) protocol. When transmitting messages devices use an SSL handshake with 2048-bit RSA keys to encrypt the socket connection to Pando servers. The infrastructure supports the sync of RSA public keys. To further enhance security OWASP certificate pinning has been implemented and access to Pando servers is only possible via SSH keys.

Step 2: 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?

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?

Pando operates a Client-Server model – sharing data, including personal patient data, over SSL encrypted links (256-bit) using Internet connections provided by Trust Wi-Fi (when clinicians are roaming on-site) or 3G/4G/5G. Data is securely transmitted, processed and stored on the Pando infrastructure. Retention is governed by the appropriate retention schedules. Please refer to Pando Data flows.

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)?

Pando is designed to be used by trained healthcare professionals in their clinical workplace (e.g. clinic, hospital, care home etc.).

Pando do not have a direct relationship with the data subject and the data subjects have as much control over their data when their clinician uses Pando as they do in any other situation where their Article 9 data is handled by their healthcare provider. The stipulated and expected use is instant messaging not as the core record of data for the Data Controller so the data is not retained for a significant duration.

Patients would expect their data to be processed as part of their ongoing care and Pando is a tool that assists healthcare professionals.

It is important to note that Pando is not the data controller – the data controller is the employer of the user (e.g. clinic, GP surgery, hospital, care home etc.). They will process data using the appropriate legal pathway which will be under Article 6.1d, 6.1e, 9.2 h and will include some children's data and some data about vulnerable adults.

Pando is owned by Pando Ltd who are registered with the ICO and have appointed a Data Protection Officer (DPO).

Pando is hosted on London Cluster's secure ISO27001 certified AWS servers.

Pando submitted DSP Toolkit in March 2019 and has Certification including Cyber Essentials.

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. Who 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?

- Engagement with relevant IG managers/CIO/CCIO at Trust with relevant team members from Forward Clinical Ltd.
- Engagement with Forward Clinical Ltd (app developer and service provider)
- Consultation is performed via internal team meetings, discussions with our initial NHS consultant users, reviewing the service provider's ISMS (Information Security Management System), Information Security Policy, Privacy Policy and SLAs (Service Level Agreements)/EULAs (End User License Agreements) and discussing technical requirements with the service providers to seek relevant assurances.
- Maintenance of information assets register and information security risk assessment and clinical hazards log.

Step 4: Assess necessity and proportionality

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?

- Pando are not the data controllers and are not processing any personally identifiable data. Where clinicians process data as controllers the legal basis would be Article 6.1d, 6.1e and 9.2h.
- Other methods of communicating / processing are likely to be fundamentally secure than using the Pando App – e.g. commercial Apps, faxes, generic email etc.
- Individuals will be informed about the use of Pando via communication directly from their clinician and via privacy notices. Clinicians must use the Pando App as directed by the IG teams within their individual Trusts and adhere to the good practice embedded into the end user agreement.
- Good practice in terms of data quality and minimisation is achieved via training and awareness and data resides on UK servers.
- The Pando development team are fully versed in the principles of 'privacy by design and default'.

Step 5: Identify and assess risks

Included below is a summary of the key privacy risks and impacts as related to the use of Pando. At all times Pando maintain an up to date information assets register, information security risk assessment and Hazards Log in compliance with SCCI0129.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/corporate risk
Staff mobile devices lost or stolen	Confidential PID made public and/or vulnerable individuals targeted by criminals.	Confidential PID made public and/or vulnerable individuals targeted by criminals.	Confidential PID made public and/or vulnerable individuals targeted by criminals.
PID digital records intercepted over internet connections	As above	As above	As above
PID digital records stolen from server platform	As above	As above	As above

Step 6: Identify measures to reduce risk

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation**: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Staff mobile devices lost or stolen – subset of PID digital records no longer secured	(1) No PID stored permanently on individuals' devices- images, tasks, patient profiles are at all times pulled down from our servers. Encrypted at rest and in transit. (2) PIN code lock-down of all mobile devices at 15 minutes maximum. Time out cannot be changed by user. (3) Remote Wipe function is included in common Exchange/ActiveSync environments, free on iOS/Android and EMM (Enterprise Mobile Management) systems are also available.	(1) Risk significantly reduced (2) Risk reduced (3) Risk significantly reduced	Solutions are justified, compliant and proportionate responses to the aims of the project.
PID digital records intercepted over internet connections	(1) Server Side Encryption (SSE), using 256-bit Advanced Encryption Standard (256-bit AES) in transit and at rest. (2) In transit data is encrypted and transferred via HTTPS (TLS 1.2 min) protocol. When transmitting messages devices use an SSL handshake with 2048-bit RSA keys to encrypt the socket connection to servers. Also supports the sync of RSA public keys. To further enhance security - OWASP certificate pinning implemented and access to Pando servers is only possible via SSH keys. (3) Strong Password policy enforced.	(2) Risk significantly reduced (3) Risk significantly reduced	Solutions are justified, compliant and proportionate responses to the aims of the project.

PID digital records stolen from server platform	(1) Insider-hacking threat eliminated; no readable PID by any system admin or developer ('data privacy by default' methodology) if an unauthorised database extraction occurs. (2) Internet-based hacking threat significantly reduced by SPI and application based firewall (layer-7), automated account lockouts (security policy) after three failed attempts, strong password enforcement (security policy) and AES-256 server data encryption. (3) Regular penetration testing carried out for both servers and smartphone application.	(1) Risk eliminated (2) Risk significantly reduced	Solutions are justified, compliant and proportionate responses to the aims of the project.

Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By
Staff mobile devices lost or stolen	(1) All data encrypted at rest and in transit. No images, tasks, patient details stored on the device. (2) PIN code lock-down of all mobile devices is mandatory. (3) Remote Wipe function is included in Exchange/ActiveSync environments, free on iOS/Android and EMM (Enterprise Mobile Management) from Trust may be deployed.	CEO PM HoI DPO

PID digital records intercepted over internet connections	(1) Server Side Encryption (SSE), using 256-bit Advanced Encryption Standard (256-bit AES) in transit and at rest. (2) In transit data is encrypted and transferred via HTTPS (TLS 1.2 min) protocol. When transmitting messages devices use an SSL handshake with 2048-bit RSA keys to encrypt the socket connection to servers. Also supports the sync of RSA public keys. To further enhance security - OWASP certificate pinning implemented and access to Pando servers is only possible via SSH keys.	CEO PM HoI DPO
PID digital records stolen from server platform	(1) Insider-hacking threat eliminated; no readable PID by any system admin or developer ('data privacy by default' methodology) if an unauthorised database extraction occurs. (2) Internet-based hacking threat significantly reduced by SPI and application-based firewall (layer-7), automated account lockouts (security policy) after three failed attempts, strong password enforcement (security policy) and AES-256 file-level server data encryption.	CEO PM HoI DPO

Ongoing Review: Integrate the DPIA outcomes back into the project plan.

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
(1) All data encrypted at rest and in transit. No images, tasks, patient details stored on the device. (2) PIN code lock-down of all mobile devices is mandatory. (3) Remote Wipe function is included in Exchange/ActiveSync environments, free on iOS/Android and EMM (Enterprise Mobile Management) from Trust may be deployed.	Actions completed by Forward Clinical Ltd.	CEO PM HoI DPO

Optional remote wipe function (Trust's EMM – Enterprise Mobile Management) enabled and tested on higher-risk end-user devices.	To be confirmed with NHS Trust. Remote closing of account available via Pando dashboard, 24/7 support available.	
(1) Server Side Encryption (SSE), using 256-bit Advanced Encryption Standard (256-bit AES) in transit and at rest. (2) In transit data is encrypted and transferred via HTTPS (TLS 1.2 min) protocol. When transmitting messages devices use an SSL handshake with 2048-bit RSA keys to encrypt the socket connection to servers. Also supports the sync of RSA public keys, ensuring high levels of encryption. To further enhance security - OWASP certificate pinning implemented and access to Pando servers is only possible via SSH keys. (3) Strong Password policy enforced.	Completed	CEO PM
(1) Insider-hacking threat eliminated; no readable PID by any system admin or developer ('data privacy by default' methodology) if an unauthorised database extraction occurs. (2) Internet-based hacking threat significantly reduced by SPI and application based firewall (layer-7), automated account lockouts (security policy) after three failed attempts, strong password enforcement (security policy) and AES-256 file-level server data encryption.	Most recent penetration testing of both application and entire infrastructure completed 9.4.18.	CEO PM

Contact point for future privacy concerns

Measures approved by Data Protection Officer dpo@hellopando.com