Forward Health

Data Protection Impact Assessment

Version 1.7 - 15.05.2018

Version	Date	Author	Reason for amendment
1.0	20.04.2017	Mr Stephen Bromham	Original authorship
1.1	26.09.2017	Dr Lucinda Scharff	Update
1.2	19.10.2017	Dr Lucinda Scharff	IG toolkit submission
1.3	15.12.2017	Dr Lucinda Scharff	Update
1.4	22.01.2018	Dr Lucinda Scharff	Review, minor changes made
1.5	05.02.2018	Dr Lucinda Scharff	To reflect new changes to enable access to data for audit/SI purposes.
1.6	20.02.2018	Dr Lucinda Scharff	To reflect changes to MIM/database.
1.7	15.05.2018	Dr Lucinda Scharff	Pre GDPR review

Introduction

This document details the data protection impact assessment carried out by Forward Health with regards to the use of Forward 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 Forward as a mobile application within (Insert name of organisation) only. It refers to the current data protections laws as they stand, although will take into consideration incoming change to the regulation and how this may affect this assessment.

Forward Health 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 information flow.

3. Identify data protection and related risks.

4. Identify data protection solutions to reduce or eliminate the risks.

5. Sign off the outcomes of the DPIA.

6. Integrate data protection solutions into the project.”[1]

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 – identical patient information is collected – only managed more efficiently and in a structured manner using the Forward Health app for mobile devices.
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	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 that people would consider to be private.	information security will be deployed.
Will the project require you to contact individuals in ways that they may find intrusive?	No

Step one: Identifying 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).

Forward is a smartphone application and communication tool for clinical teams. Forward 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 Health 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, 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.

Forward Health additionally provides the Trust with high-levels of technical data security assurance such as high levels on 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 Forward Health servers. The infrastructure supports the sync of RSA public keys. To further enhance security OWASP certificate pinning has been implemented and access to Forward servers is only possible via SSH keys.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Forward Health 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. Data is securely transmitted, processed and stored on the Forward Health infrastructure. Please refer to Forward Health Data flows, attached.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. You can use consultation at any stage of the DPIA process.

- NHS IG Toolkit approach (Forward has Level 2 IG Toolkit Certification)
- Maintenance of information assets register and information security risk assessment
- Maintenance of clinical hazards log
- Engagement with relevant IG managers/CIO/CCIO at Trust with relevant team members from Forward Health
- Engagement with Forward Health (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 and SLAs (Service Level Agreements)/EULAs (End User License Agreements) and discussing technical requirements with the service providers to seek relevant assurances.

Step three: Identify the privacy and related risks
Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Note: 'PID' – Personal Identifiable Data

Included below is a summary of the key privacy risks and impacts as related to use of Forward Health, At all times we 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.	In breach of: NHS IG Toolkit guidelines, NHS Confidentiality Code of Conduct, Data Protection Act 1998; and support compliance to the Access to Health Records Act 1990.	Potential fines, loss of credibility and damage to reputation.
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 four: Identify privacy solutions

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(s)**	**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 can not 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	(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	(1) Risk significantly reduced	Solutions are justified, compliant and proportionate responses to the

connections	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 Forward servers is only possible via SSH keys. (3) Strong Password policy enforced.	(2) Risk significantly reduced (3) Risk significantly reduced	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.

Step five: 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 LS
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 Forward servers is only possible via SSH keys.	CEO PM HoI LS
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 LS

Step six: 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 Health.	CEO PM HoI LS
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 Forward 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	Completed	CEO PM

enhance security - OWASP certificate pinning implemented and access to Forward servers is only possible via SSH keys. (3) Strong Password policy enforced.		
(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
Head of Information Dr Lucinda Scharff

Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Linking the DPIA to relevant data protection law and GDPR

Answering these questions during the DPIA process will help to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act. Please include the answers and reasoning behind them in your submission to the ISAG.

1. **Personal data shall be processed fairly and lawfully**

Have you identified the purpose of the project?
Yes, these are documented within the DPIA.

How will you tell individuals about the use of their personal data?
Users - on registration users are asked to agree to our privacy policy, available to them to read at that point. Our privacy policy is at all times available via the app, our website or on request. Users will be informed of any significant change that takes place.
Patients - there is an expectation that those with a duty of care to a patient will share relevant clinical information with others that also share this duty of care. Should the organisation require any documentation to assist patients in understanding Forward and how their information is shared, Forward Health will support the organisation in providing these.

Do you need to amend your privacy notices? Amended pre GDPR.

Have you established which legal conditions for processing apply?
Users - explicit consent 6(a)
Patients - legal obligation of the controller 6(1)(c) and special category health data 9(2)(h).

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
User consent is collected by opt in on registration. Users are made aware that they can withdraw this consent at any time but this may impact upon the service Forward Health is able to provide to them. A record of their consent withdrawal will need to be held to prevent unlawful processing of their data in the future.

Will your actions interfere with the right to privacy under Article 8? No

Have you identified the social need and aims of the project? Yes, to provide clinical teams and healthcare professionals with an ability to securely communicate via mobile, with the aims of providing more efficient communication, reducing delays and ultimately providing better patient care, and a better working environment.

Are your actions a proportionate response to the social need? Yes.

2. **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

Does your project plan cover all of the purposes for processing personal data?
Yes

Have you identified potential new purposes as the scope of the project expands?
Not at this time. If any significant change is planned to the ways in which data is collected, processed, or new categories of data are included then a new DPIA will be required.

3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

Is the quality of the information good enough for the purposes it is used?
Yes, all information is entered either by the user themselves, about themselves, or about the patients they have a duty of care to.

Which personal data could you not use, without compromising the needs of the project?
We have no planned requirement for automated export or transfer of historic personal data of any patient from the NHS spine or Trust ERP systems.

The clinicians create their own associated notes, messages shared only with those involved in delivering direct care to the patient plus general observations/reminders – sometimes shared with authorised colleagues also using Forward. All data is manually entered by end- users, replacing insecure handwritten notes and/or non-vetted third party smartphone apps/services.

Again - the project aim is quite specific and limited, i.e. for the Trust to safely and secure share patient information/notes on clinicians' mobile devices (activities/messages/profiles) – only with authorised colleagues who use the same approved platform from Forward.

4. **Personal data shall be accurate and, where necessary, kept up to date.**

If you are procuring new software does it allow you to amend data when necessary?
User data can be updated either within Forward or by contacting our team via email or the support line. Patient data can be amended by users within the application.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

A full audit trail with username plus date/time stamp of uploads and communications authenticates the origin of all personal data. Ensuring the factual accuracy of any data entered by an end-user clinician is not within the scope of this project.

5. **Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.**

What retention periods are suitable for the personal data you will be processing?
Data is stored for five years, for the purpose of providing an audit trail or evidence in the case of an SI, unless a legal request is made to delete this data prior to that date.

Are you procuring software that will allow you to delete information in line with your retention periods?
Yes, data is tagged with an expiry date such that deletion will occur automatically after five years.

6. **Personal data shall be processed in accordance with the rights of data subjects**

Will the systems you are putting in place allow you to respond to subject access requests more easily?
Yes, data is stored hierarchically, with patients under teams, under organisations, meaning SAR will be responded to within the legal time frames required.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?
Marketing is only targeted to users on the basis of consent. Users have to actively opt in to receive marketing emails. Users are currently and will remain able to opt out simply by unsubscribing via the link in marketing emails, or on request to a Forward team member. WE will continue to provide users with information regarding updates, service changes on the basis of legitimate interests.

7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

Do any new systems provide protection against the security risks you have identified?
Yes, Forward and/or our IT infrastructure provides the following protection against our identified security risks.

(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) Server Side Encryption (SSE), using 256-bit Advanced Encryption Standard (256-bit AES) in transit and at rest.

(4) 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. To further enhance security - OWASP certificate pinning implemented and access to Forward servers is only possible via SSH keys.

(5) Strong Password policy enforced with MFA for all Forward staff.

(6) PIN code lock-down of all mobile devices is mandatory.

(7) Remote Wipe function is included in Exchange/ActiveSync environments, free on iOS/Android and EMM (Enterprise Mobile Management) from Trust may be deployed.

What training and instructions are necessary to ensure that staff know how to operate a new system securely?
It is expected that all staff with NHS or trust domain email addresses will undergo mandatory information governance training on an annual basis. Forward is designed to be simple and intuitive for the user, however we will provide onboarding documentation and support where needed, including a 24/7 support line. Further support and training will be agreed with the organisation.

8. **Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

Will the project require you to transfer data outside of the EEA?
No, all data is stored within the London AWS Cluster, there are no transfers outside of the UK or EEA.

If you will be making transfers, how will you ensure that the data is adequately protected?
N/A