|  |  |
| --- | --- |
| Document filename: | **111 Online Private Beta Privacy Impact Assessment** |
| Project / Programme | **Domain B** | Project | **111 Online** |
| Project Manager | **Chris Fleming** | Status | **[Draft]** |
| Author | **Chris Fleming** | Version | **0.6** |
| Sponsor | **Dr Alastair Pickering** | Version issue date | **[Publish Date]** |

**111 Online Privacy Impact Assessment**

# Document management

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** |
| 0.1 |  |  |
| 0.2 | 20/11/16 | Additional detail and cross-references to security matrix added. |
| 0.3 | 14/12/16 | Updated to align with PN |
| 0.4 | 20/12/16 | Final amends before send to CG |

**Reviewers**

This document must be reviewed by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reviewer name** | **Title / Responsibility** | **Date** | **Version** |
| Pete Spence | IG Manager | 20/12/16 | 0.2 |
| Steve Bellerby | Deliver Manager | 21/11/16 | 0.2 |
| Mandy Williams | Programme Head | 21/11/16 | 0.2 |
| Tim Coates | Lead TA | 21/11/16 | 0.2 |
| Chris Fleming | Programme Head | 21/11/16 | 0.2 |
| Alastair Pickering | Clinical LeadDomain B | 21/11/16 | 0.2 |

**Approved by**

This document must be approved by the following people:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Signature** | **Title** | **Date**  | **Version** |
| Prof Martin Severs |  | Medical Director and Caldicott Guardian, NHS Digital |  |  |

**Document Control:**

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

**Contents**

[1. Document management](#_gjdgxs)

[2. Project Outline](#_tyjcwt)

[3. Initial Impact Questions](#_3dy6vkm)

[4. Data Environment Questions](#_1t3h5sf)

[5. Data Transfer and Reporting](#_3whwml4)

[6. Additional Legal Considerations](#_2grqrue)

[0. Glossary](#_28h4qwu)

# Project Outline and Data Flows

NHS 111 online is a patient facing service to enable users to self-serve part or all of the NHS 111 triage process, then be connected to the service they need. The purpose of this initiative is to reflect the growing demand for NHS 111 telephone services and to work on implementing local channel shift before the volume of calls becomes unsustainable.

## User journey

The user journey is as follows:

1. Users arrive at the service.
2. User confirms not an emergency situation.
3. User provides details of gender and age.
4. User identifies the symptom closest to what they have from a list or search.
5. User answers a series of questions and answers relating to their symptom that match the clinically approved pathways algorithm.
6. User is presented with a disposition.
7. (For some dispositions) User has option to look up a service. In which case they provide post code.
8. (For some services) User has option to provide their personal details and be called back by that service.

Where a provider is required to be notified of an individual’s outcome of triage in order to call them back, the service shall ask the individual to provide personal identifiable information (Name, DOB, Address, Telephone number) before the data is sent to the provider. The service uses ITK messaging (over TLS Authentication) to dispatch message to the provider. A copy of the ITK message data is then encrypted in a table for audit purposes.

## Data collection

We collect data across the following categories:

1. **Analytics**: data on the pages and links the user clicks on when travelling through the website.
2. **Non functional**: we log extremely granular data on performance such as uptime and perform load testing to ensure resilience
3. **Demographic**: data the user inputs in order to be able to use the service i.e. be triaged and get a referral
4. **Pathways**: the website interprets the pathways clinical triage dataset and transforms it into a digital service; we collect the answers users provided to pathways questions (yes,no, don’t know) and the disposition they receive
5. **Survey**: there are a number of ways users can feedback on the site. Data is captured by an optional questionnaire that will use Verint survey tool.

## Scope of PIA

The scope of this PIA is to cover the **111 Online service private beta**. The private beta is going to run Mar-Apr and will be targeted at reaching 5000 users. To ensure a controlled Private Beta test is achieved, 3 CCGs have been chosen in West Yorkshire: Leeds North, Leeds South and East, and Leeds West. The trial areas have good access to Primary Care in and out of hours along with suitable additional services such as Walk in Centre or Minor Injury Unit, to ensure that users of 111 Online could be offered a range of services that are accessible.

##  Legal basis

NHS England is directing NHS Digital under the Health and Social Care Act s274 system delivery function for the service; and are directing NHS Digital to collect data under s254 for the service. The data disseminated is confidential patient information which flows to local health services for the purposes of direct patient care. It comprises NHS Pathways questions and answers plus the required disposition and local instantiation of that disposition.

While there are currently no plans for dissemination for secondary purposes, if this position changes in the future then any such dissemination would be under s261 of the Health and Social Care Act. This sets out tight controls around dissemination including restricted purposes and a requirement for a specific legal basis in order to disseminate.

## Risks (Inherent or Residual)

For each risk, please state the;

* Description
* Mitigating actions
* Treatment (Transfer, Accept, Reduce, Avoid)
* Residual Score – *See* [*HSCIC Tracking Database*](https://nww.tdb.nhs.uk/ifhtracking/Content/Login.aspx) *for Impact and Probability Scoring*
* How the risk(s) will be tracked and where

**Risk log**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref** | **Area** | **Owner** | **Description** | **Possible impacts** | **Score** | **Mitigating actions** | **Owner** | **Completion date** | **Last reviewed** | **Resid****risk** |
| ONL52 | Security and privacy | Chris Fleming | Deanonymisation of data due to possible matching with survey data. | Compromise of patient privacy | Med | Lo | Strict access to PCD. A System Level security policy has been completed by the NHS Digital 111 team.  | Steve Bellerby | Done | 20/12/2016 | Lo |
| ONL53 | Security and privacy | Chris Fleming | ITK messages intercepted or sent to wrong endpoint | Loss of patient data. Additional cost, delays, harm to NHS Digital reputation. (clinical risk noted above) | Med | Lo | All data to be encrypted in transit using suitable levels of protection. - RSA 2048 - TLS1.2 - AES 256 - SHA256 | Steve Bellerby | Done | 20/12/2016 | Lo |
| ONL54 | Security and privacy | Chris Fleming | Masquerading of User Identity by Insiders | Limited | Lo | Lo | No appropriate mitigations. | N/A | N/A | 20/12/2016 | Lo |
| ONL55 | Security and privacy | Chris Fleming | Masquerading of User Identity by Contracted Service Providers | Limited | Lo | Lo | The 111 service will have no connection to any server instance not supported by NHS Digital staff. | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL56 | Security and privacy | Chris Fleming | Masquerading of User Identity by Outsiders | Disruption to service | Hi | Hi | There are limited controls to stop false information from being automatically updated onto the system resulting in Denial of Service (DOS) of 111 Online Service providers. This would be the electronic equivalent of 111 nuisance calls. Akamai CDN rate control is in place to control for DDOS. | Steve Bellerby | Done | 3/12/2016 | Hi |
| ONL57 | Security and privacy | Chris Fleming | Unauthorised Use of an Application | The front end has no user credentials. | Lo | Lo | Successful penetration testing has been carried out | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL58 | Security and privacy | Chris Fleming | Introduction of Damaging or Disruptive Software | Disruption to service | Lo | Hi | Users are unable to load files into the application. Anti Virus controls are in place. Execution control software is in place. | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL59 | Security and privacy | Chris Fleming | Misuse of System Resources | Denial of service attack. | Lo | Med | (i) Data traffic monitoring(ii) Business continuity plans(iii) Akamai CDN providing WAF and Rate Control. | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL60 | Security and privacy | Chris Fleming | Communications Infiltration | Data breach | Lo | Med | Due to nature of system there would be limited value in infiltration of new messages. Such message could be created via the web interface. Mitigations: (i) Firewall(s) (ii) Penetration testing (iii) Encryption (iv) Akamai | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL61 | Security and privacy | Chris Fleming | Communications Interception | Data breach | Lo | Med | Interception of communications is unlikely however is possible but encryption in place would impede the access of data. Mitigations: (i) Firewall(s) (ii) Penetration testing (iii) Encryption (iv) Akamai | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL62 | Security and privacy | Chris Fleming | Communications Manipulation | Data breach | Lo | Med | The manipulation of data in transit would have limited value. Mitigations: (i) Firewall(s) (ii) Penetration testing (iii) Encryption (iv) Akamai | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL63 | Security and privacy | Chris Fleming | Repudiation | Wrong information being passed to healthcare service | Lo | Med | ITK Messaging is used to verify this information. (ie; the ability to verify message content is unaltered between sender and recipient). Revalidation of details by clinicians.  | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL64 | Security and privacy | Chris Fleming | Communications/Systems Failure | Limited impact for private beta | Med | Lo | If there is a catastrophic failure of the service, it will be rebuilt in the same or a different Microsoft Azure datacentre within England within 24 hours. Should the service be turned off, users coming to the service will be directed to ring 111 | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL65 | Security and privacy | Chris Fleming | Embedding of Malicious Code | The embedding malicous code through the front end would cause significant damage. | Lo | Hi | Users are unable to upload files. Security controls. See 111 Online Security Plan | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL66 | Security and privacy | Chris Fleming | Accidental Mis-routing | Dispatch of the ITK message to wrong endpoint | Med | Hi | Extensive testing of ITK prior to go-live completed. Local services alerted. ITK message spec limits this risk. | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL67 | Security and privacy | Chris Fleming | Operations Error | Business process or operations error resulting loss of data. | Med | Med | 111 Team have completed a Service Level Security Plan to govern access to data. | Steve Bellerby | Done | 3/12/2016 | Lo |
| ONL68 | Security and privacy | Chris Fleming | Collecting data without directions in place from NHS England for the work | Collecting patient information ultra vires; will not have any impact on actual safety of patient data but any violation of DPA could damage brand / reputation. | Lo | Hi | Directions drafted; further drafting tweaks required before clearance by Chair’s action. | Chris Fleming | 17/02/2017Approved | 20/12/2016 | Med |
| ONL69 | Security and privacy | Chris Fleming | Compromise of feedback survey data | Loss of personal information | Med | Med | The Verint tool is hosted within the Savvis data centre in Slough and is ISO27001 compliant. Full statement of Verint privacy polices available on request. | Jeanette Attan | Done | 20/12/2016 | Lo |

All risks are tracked via 111 online risk Register. (Contact chris.fleming@nhs.net for details).

# Initial Impact Questions

*The answers to some of the following questions are check boxes. To tick one of these boxes, double click on the box and select the “Checked” option.*

**Explanatory note:** NHS 111 online private beta has been built on NHS Choices infrastructure. However, users’ journeys of the beta phase will be restricted to the 111 site.

## Does logging into an NHS Choices user account affect this solution at all?

☐ Yes ☒ No

## Does the user enter any data into the application?

☒ Yes ☐ No

## Is any personally identifiable information captured from the user as part of their journey throughout 111 online?

☒ Yes ☐ No

Name, DOB, Address, Postcode, Telephone number, Age, Gender

# Data Environment Questions

## Is this proposed usage similar to anything currently in use, or previously used by NHS Choices infrastructure? (If yes, please stipulate what and where it is used)

☒ Yes ☐ No

Yes, the service is similar to the Symptom Checkers that were on the NHS Choices service until closure. There are some differences in terms of functionality and technical architecture.

## Would this proposed usage require tracking of the user to allow for retrieval of this information by themselves or another party at a later date?

☒ Yes ☐ No

## If Yes, please state why the tracking is required:

* Analytics: data on the pages and links the user clicks on when travelling through the website to help us understand behavior and improve the site
* Non functional: data on performance such as uptime, load, scaling to ensure resilience
* Demographic: to enable the user to be triaged and get a referral
* Pathways: the website interprets the pathways clinical triage dataset and transforms it into a digital service; we collect the answers users provided to pathways questions (yes,no, don’t know) and the disposition they receive
* Survey: there are a number of ways users can feedback on the site. This helps us improve the service.

## Would the proposed usage be able to track where the user has visited prior to or after using this functionality?

☒ Yes ☐ No

## If Yes, please state why the tracking is required:

Prior to the user arriving at the service, we will be able to track where they have arrived at the site from using analytics. This is important for understanding complete user journeys and how users are navigating to the site.

When a user completes a journey with a referral, we will be able to track the onward journey of the patient via their ITK message via our partners in Leeds CCGs. This will be explained to users in the ITK referral page and privacy policy. Ensuring that users’ care has appropriately been transferred is a clinical safety necessity for the purposes of direct care.

Tracking also creates a record which is necessary for complaint management.

## Does the proposed usage involve the handling or processing of any personal data, as the term is used within the Data Protection Act (DPA)?

☒Yes ☐ No

If yes, what attributes does it capture?

☒ Email address *(optional) (for questionnaire)*

☒ First Name

☒ Surname

☒ Full Postcode

☒ I.P Address

☒ Telephone/Mobile number

☒ Age

☒ Date of Birth

☐ Picture, photograph, video, audio-tape or other images of the person

☐ The person’s NHS number or other local identifiers

☒ Other (Please specify)

Question and answer information based on the users’ symptoms

## Will NHS 111 process the data provided by the end user with data from another source (including information held or created by NHS 111)? If so, please specify what.

There will be a need to match data to investigate user journeys and evaluate the impact of this new digital service on local services. Any data matching will only be done at aggregate and anonymised level. Deanonymisation due to small datasets is an identified risk which will be mitigated by strict access to the data.

In the case of a clinical incident, there may be a need to match a user’s ITK referral message with their session analytics. This is explained to the user in the privacy notice.

## What is the projected number of users per annum / per lifecycle (please specify) for this project?

For private beta circa 5000 participants. Only a small subset of these who are offered appropriate dispositions at appropriate times could be expected to provide identifiable data.

## What is the data retention period for the data collected by this proposed usage and is there any expected legal obligation to archive the information beyond the expected data retention period?

The data retention period is 8 years, as per NHS Digital Retention Schedule: <http://systems.digital.nhs.uk/infogov/iga/resources/rmcop/index_html>

Data to be reviewed and if no longer needed destroyed after this period.

## To ensure that this information is being processed in accordance with the Data Protection Act, we need to understand the purpose of collecting this information. How will it be used once collected?

The primary purpose of collecting personal data is to enable us to provide them with relevant clinical algorithms, and refer the user to the correct service. Data will also be used to help drive service improvement across the 111 service (both Telephone and online) and at aggregate level will be used to understand the impact of the pilot on local services.

# Data Transfer and Reporting

## Identify all the parties who will be (i) receiving some or all the information gathered or obtained (ii) why they will be receiving it (iii) how long they will be receiving it for

NHS Digital will be hosting information gathered during user journeys and will be storing ITK messages for audit purposes. For details of where the data will be stored and the controls in place please see complementary document NHS 111 Online Security Plans.

In addition, West Yorkshire 111, West Yorkshire primary OOH service, and West Yorkshire Emergency Dental Service, will receive individual ITK referral messages for the length of the private beta - December 2016 to February 2017.

NHS England will receive report data on the service but not identifiable individuals.

## Who are the Stakeholders for this project, including all parties sponsoring this work?

Deborah El Sayed, Director of Digital and Multi-Channel, NHS England (SRO)

Chris Fleming, Programme Head, NHS Digital

Mandy Williams, Programme Head, NHS Digital

James Hawkins, Executive Director of Health Digital Service, NHS Digital

Keeley Townend, Yorkshire Ambulance Service

## How is the information transferred between different parties transmitted?

For example, how the user submits their data, or as it is transferred between NHS Choices and a third party solution provider

**N.B.** Any transfer mechanism in the left hand column above is considered to be insecure; using a transfer mechanism for this may impact the approval of this PIA. The right hand column provides a number of alternative mechanisms that should aid approval.

☐ HTTP ☒ HTTPS (SSL/TLS)

☐ Email ☐ AES Encrypted Email attachment

☐ RSYNC ☐ SCP

☐ FTP ☐ SFTP/ FTPS

☐ Fax ☐ Safehaven Fax

☐ SMB ☐ AES Encrypted DVD

☐ Hard Copy (Post) ☐ Hard copy (Courier)

☐ Other (Please specify) ☐ Secure email transfer nhs.net to nhs.net

☐ Secure API tunnel

## Where information is being transmitted, what justification and mitigation is being provided to prevent data interception?

Information is being to health services in the private beta location to support patient care. Interception is prevented by endpoints being secured using digital certificates over TLS.

## Where data is being held on third party systems on behalf of NHS 111, how will the data be secured to prevent unauthorised use or access?

In summary:

* The application is hosted on MS Azure and requires two factor authentication to access it.
* The Azure environment complies to ISO27001 standard. Microsoft are currently validating the UK centres to this – all other azure Datacentres meet these criteria.
* The data shall at all time reside in physically secure Datacentres that meet industry good practice controls.
* PCD Data written to the database will be encrypted asymetrically by the application. Access to the data to only be possible using credentials held outside of Azure.
* We have contractual confirmation and internal control from Microsoft. No access to data by Datacentre (Microsoft Azure) employees.

Full details of the security controls in place around the data for NHS 111 are given in the complementary document NHS 111 Online Security Assurance Matrix. Available on request.

## Assuming that the end user has submitted the data from within the UK, does the information become transmitted or transferred outside of the UK Geographic boundaries at any point?

☐ Yes ☒ No

Azure hosting is in UK datacentres (England/Wales)

# Additional Legal Considerations

Additional legislation can affect a decision on how private or personal information may be processed within the UK.

For example:

* Data Protection Act 1998
* Human Rights Act 1998
* Regulation of Investigatory Powers Act 2000
* Privacy and Electronic Communication Regulations 2003
* Data Retention Regulations (EC Directive) 2007
* Common Law Duty of Confidence
* Statute Code, e.g. ICO code of practice

## Does this solution involve any activities (including data handling), that are subject to a form of statute other than the DPA, such as any of the examples above? (If Yes, please stipulate which)

☒ Yes ☐ No

ICO Code of Practice; CLDOC.

## Is it envisaged that this solution would require a change to the Privacy and Security policies of NHS 111?

☐ Yes ☒ No

## If any data is not being held on NHS Choices infrastructure, the hosting company must be placed under data handling contractual restraints. Please verify this is the case. If not, you must ensure this is arranged.

☐ Yes ☒ No

NHS 111 Online is a public facing digital service; requiring a scalable flexible architecture to enable us to deploy code quickly and ensure a resilient service. A key decision was made early in the project to host on NHS Choices Infrastructure in order to meet these goals.

Because the service is being held on NHS Choices infrastructure; which is held on Microsoft Azure, the same controls will be in place as for NHS Choices data. So there are no legitimate means by which Microsoft employees can access the data and that technical controls have been put in place to ensure this. Microsoft in this case are not handling the data in that is they do not have any direct access. See 5.5 above.

## What is the process through which a user or organisation can request the removal of submitted information or to gain access to their submitted information?

Users will be able to obtain contact details via the Terms & Conditions for the service. Messages will be sent to an NHS Choices managed mailbox and then be flagged to the team. If a user wishes to see all the information held on them by this system they can make a subject access request under the Data Protection Act. If a user wants to have their information removed then if they contact us we will do this. This latter action goes beyond what we are legally required to do.

## Once the information has been collected, who will have access rights to it and what assurance is in place to verify the suitability of the 3rd party?

Access is restricted to certain 111 online team members and relevant infrastructure members. Access will follow NHS Digital’s policy for controlling access to confidential information which provides tight controls on who can access such information and for what purposes. Microsoft do not have access to the data due to the levels of encryption and are contractually prohibited from accessing it. Full details of authentication and authorisation of users who will have access to data is available on request.

# Glossary

|  |  |
| --- | --- |
| **Term** | **Description** |
| DPA | Data Protection Act |
| DVD | Digital Versatile Disc |
| EC | European Community |
| FTP | File Transfer Protocol |
| FTPS | File Transfer Protocol (Secure) |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol (Secure) |
| ICO | Information Commissioner’s Office |
| NHS | National Health Service |
| RSYNC | A software application for synchronising files across systems for Unix and Windows |
| SCP | Secure Copy Protocol |
| SFTP | Secure File Transfer Protocol |
| SMB | Server Message Block |