

Data Protection Impact Assessment

(DPIA) IGAR (3250, 4084, 4553) 5191

NHS Breast Screening Programme Patient Communications

Document Status: Approved

|  |  |
| --- | --- |
| Version: | 2.5 |
| Ratified by: | Information Governance Group |
| Date ratified: | 08/08/2022 |
| Owner (title): | Simon Stewart – Senior Information Governance Manager |
| Accountable director (title) | Kevin Winter – Associate Director of Information Governance |
| Date issued: | 23/08/2022 |
| Review date: | 23/08/2023 |
| Target audience: | All Staff |
| Freenet: |  |

# Version Control

## Template Version Control Sheet

*Do not amend this table when implementing a local version, use ‘Implementation Version Control Sheet’ below.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Name | Status | Comment |
| 2.0 | 23/08/2021 | Kevin Winter – Associate Director of Information Governance | Pilot | Revision of DPIA template to reflect changes in data governance, privacy and technology. |
| 2.1 | 27/08/2021 | Kevin Winter – Associate Director of Information Governance | Pilot | Minor amendments. |
| 2.2 | 17/09/2021 | Kevin Winter – Associate Director of Information Governance | Pilot | Minor amendments. |
| 2.3 | 17/09/2021 | Kevin Winter – Associate Director of Information Governance | Pilot | Minor amendments. |
| 2.4 | 07/06/2023 | Ben Tunmore, Head of Information Governance (Consultancy) | Final | Technical guidance updated |
| 2.5 | 28/11/2023 | Kevin Winter – Associate Director of Information Governance | Final | Added in requirement for risks to be incorporated into project plans or local risk management processes. |

## Implementation Version Control Sheet

*Local implementation version control to be used by services completing the template to track their revisions.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Name | Status | Comment |
| 0.1 | 13/03/2024 | Kenneth Blake – Assistant Operations Manager, London Breast Screening Programme Administration Hub | Draft | Preliminary information added to document |
| 0.2 | 10/04/2024 | Ben Tunmore, Head of Information Governance (Consultancy) | Draft | Added comments and track changes for review |
| 0.3 | 11/04/2024 | Kenneth Blake – Assistant Operations Manager, London Breast Screening Programme Administration Hub | Draft | Document amended and track changes/comment responses for review |
| 0.4 | 11/04/2024 | Ben Tunmore, Head of Information Governance (Consultancy) | Draft | Added comments and track changes for review |
| 0.5 | 12/04/2024 | Kenneth Blake – Assistant Operations Manager, London Breast Screening Programme Administration Hub | Draft | Added comments and changes for review/approval |
| 0.6 | 16/04/2024 | Ben Tunmore, Head of Information Governance (Consultancy) | Draft | Minor amendments to 6.1, 6.11 & 11. |
| 1.0 | 16/04/2024 | Kenneth Blake – Assistant Operations Manager, London Breast Screening Programme Administration Hub | Final | Amendments reviewed |
| 1.1 | 17/07/2024 | Kenneth Blake – Assistant Operations Manager, London Breast Screening Programme Administration Hub | Updated | Section 12 actions updated with outcomes as of 17/07/2024 review |
| 1.2 | 22/10/2024 | Kenneth Blake – Assistant Operations Manager, London Breast Screening Programme Administration Hub | Updated | DPIA reviewed and updated to include proposed changes to electronic GP reports via time limited PDF email link | |
| 1.3 | 16/11/2024 | Ben Tunmore, Head of Information Governance (Consultancy) | Final | Added summary to section 2.2 Purpose | |
| 1.4 | 19/12/2024 | Kenneth Blake – Assistant Operations Manager & Danielle Macpherson-Smith – Service Manager, London Breast Screening Programme Administration Hub | Updated | DPIA reviewed and updated to include proposed changes to electronic client letters via time limited PDF email link with client DOB validation | |
| 1.5 | 20/12/2024 | Ben Tunmore, Head of Information Governance (Consultancy) | Draft | Clarification comments added to sections 2.2 and 6.3. | |
| 1.6 | 17/02/2025 | Kenneth Blake – Assistant Operations Manager & Danielle Macpherson-Smith – Service Manager, London Breast Screening Programme Administration Hub | Draft | Clarification comments responded to in sections 2.2 and 6.3. | |
| 1.7 | 26/02/2025 | Ben Tunmore, Head of Information Governance (Consultancy) | Draft | Reviewed changes and responded to comments. | |
| 1.8 | 27/02/2025 | Kenneth Blake – Assistant Operations Manager & Danielle Macpherson-Smith – Service Manager, London Breast Screening Programme Administration Hub | Draft | Updated in light of review comments and feedback. Track changes for review | |
| 1.9 | 28/03/2025 | Ben Tunmore, Head of Information Governance (Consultancy) | Draft | Reviewed and marked updates in red for sending time limited links to correspondence via email/SMS. | |
| 1.10 | 28/03/2025 | Kenneth Blake – Assistant Operations Manager, London Breast Screening Programme Administration Hub | Draft | Reviewed and confirmed text in red and track change amendments as per comments received | |
| 1.11 | 28/03/2025 | Ben Tunmore, Head of Information Governance (Consultancy) | Final | Reviewed and accepted changes in sections 11 & 12. | |
|  |  |  |  |  | |
|  | | | | |
|  | | | | |

Contents

[Version Control 2](#_Toc194047461)

[Template Version Control Sheet 2](#_Toc194047462)

[Implementation Version Control Sheet 2](#_Toc194047463)

[Section 1 – Administrative Information 6](#_Toc194047464)

[1.1 Organisations 6](#_Toc194047465)

[1.2 People 7](#_Toc194047466)

[Section 2 – Details 8](#_Toc194047467)

[Section 3 – Screening Questions 17](#_Toc194047468)

[Section 4 – Data 18](#_Toc194047469)

[4.1 Personal Data – Primary data subjects 18](#_Toc194047470)

[4.2 Special Category Personal Data – Primary data subjects 19](#_Toc194047471)

[4.3 Personal Data – Secondary data subjects 20](#_Toc194047472)

[4.4 Special Category Personal Data – Secondary data subjects 21](#_Toc194047473)

[Section 5 – Legal 21](#_Toc194047474)

[Section 6 – Technical and Organisational Controls 26](#_Toc194047475)

[Section 7 – Process and Policy 31](#_Toc194047476)

[Section 8 – Data Subject Rights 34](#_Toc194047477)

[Section 9 – Supporting Documents 36](#_Toc194047478)

[Section 10 – Consultation 37](#_Toc194047479)

[Section 11 – Risks 38](#_Toc194047480)

[Risk Matrix 38](#_Toc194047481)

[Section 12 – Actions 41](#_Toc194047482)

[Section 13 – Review and Approval 43](#_Toc194047483)

[Annex 1 – Definitions 45](#_Toc194047484)

# Section 1 – Administrative Information

## 1.1 Organisations

*Provide details of the organisations involved in the project or programme.*

|  |  |  |  |
| --- | --- | --- | --- |
| 1.1.1 Controllers | | | |
| [Name](file:///C:/Users/KevinWinter/Documents/Royal%20Free/IG/Templates/DRAFT/DPIA/) | [**Information Commissioners Office (ICO) registration number**](https://ico.org.uk/ESDWebPages/Search) | [**Brief details of role**](file:///C:/Users/KevinWinter/Documents/Royal%20Free/IG/Templates/DRAFT/DPIA/) | [**Status**](#_Definitions) |
| The Royal Free London NHS Foundation Trust (RFL) | Z6460180 | Host Trust of the London Breast Screening Programme Administration Hub  The Hub delivers all administration functions for London’s 6 breast screening services, including the sending of patient communications (letters and text reminders) | Controller |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1.1.2 Processors | | | | | |
| [Name](file:///C:/Users/KevinWinter/Documents/Royal%20Free/IG/Templates/DRAFT/DPIA/) | [**Data Security and Protection Toolkit (DSPT) registration number**](https://www.dsptoolkit.nhs.uk/OrganisationSearch) | [**Brief details of role**](https://nhs.sharepoint.com/sites/RAL_InformationGovernance/Shared%20Documents/Corporate%20Information%20Governance%20Service/Templates/Data%20Protection%20Impact%20Assessment%20(DPIA)) | [**Status**](https://nhs.sharepoint.com/sites/RAL_InformationGovernance/Shared%20Documents/Corporate%20Information%20Governance%20Service/Templates/Data%20Protection%20Impact%20Assessment%20(DPIA)) | **Provider assurance completed** | **Contract in place** |
| Civica UK Limited (People Governance, Healthcare) | 8HC47  22/23 Standards Met | Processor of client communications (letter printing and text reminders transmission) | Processor | Yes | Yes |
| Funasset Ltd | 8HW72  22/23 Standards Exceeded | Partner of Civica UK Ltd and software provider of Civica ‘Smart Mail’ interface | Sub-processor | Yes | Yes |

|  |  |  |
| --- | --- | --- |
| 1.1.3 Other Stakeholder Organisations, People or Groups | | |
| [Name](file:///C:/Users/KevinWinter/Documents/Royal%20Free/IG/Templates/DRAFT/DPIA/) | **Brief details of role** | **Status** |
| NHS England (NHSE) public health commissioning and operations team | Facilitate regional healthcare commissioning and delivery across the London region, including the NHS Breast Screening Programme (NHSBSP) | Commissioner |
| London SQAS – Screening Quality Assurance Service | Regional QA service for NHSBSP that assess quality of screening programme, monitor compliance with standards, support service quality improvements and undertake regional level QA reviews | Quality Assurance |

## 1.2 People

*Provide details of the key people involved in the project or programme.*

|  |  |
| --- | --- |
| 1.2.1 Project/Programme Lead | |
| Name | Kenneth Blake |
| Organisation | Royal Free London NHS Foundation Trust |
| Job Title | Assistant Operations Manager |
| Role in Project | Project Lead |
| Contact Number | 020 3758 2495 |
| Email Address | [Kenneth.blake@nhs.net](mailto:Kenneth.blake@nhs.net) |

|  |  |
| --- | --- |
| 1.2.2 [Person completing DPIA (if different from above)](https://nhs.sharepoint.com/sites/RAL_InformationGovernance/Shared%20Documents/Corporate%20Information%20Governance%20Service/Templates/Data%20Protection%20Impact%20Assessment%20(DPIA)) | |
| Name | As above |
| Organisation | As above |
| Job Title | As above |
| Role in Project | As above |
| Contact Number | As above |
| Email Address | As above |

|  |  |
| --- | --- |
| 1.2.3 [Information Asset Owner](https://nhs.sharepoint.com/sites/RAL_InformationGovernance/Shared%20Documents/Corporate%20Information%20Governance%20Service/Templates/Data%20Protection%20Impact%20Assessment%20(DPIA))  *An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.* | |
| Name | Julia Kitteringham |
| Organisation | Royal Free London NHS Foundation Trust |
| Job Title | Director of Operations – Chase Farm Business Unit |
| Contact Number |  |
| Email Address | [juliakitteringham@nhs.net](mailto:juliakitteringham@nhs.net) |

|  |  |
| --- | --- |
| 1.2.4 [Information Asset Administrator](https://nhs.sharepoint.com/sites/RAL_InformationGovernance/Shared%20Documents/Corporate%20Information%20Governance%20Service/Templates/Data%20Protection%20Impact%20Assessment%20(DPIA)) | |
| Name | Kenneth Blake |
| Organisation | Royal Free London NHS Foundation Trust |
| Job Title | Assistant Operations Manager |
| Contact Number | 020 3758 2495 |
| Email Address | [Kenneth.blake@nhs.net](mailto:Kenneth.blake@nhs.net) |

# Section 2 – Details

*In this section you should detail, what you are doing, and why.*

|  |
| --- |
| 2.1 Context |
| The NHS Breast Screening Programme (NHS BSP) is a national population screening programme. The aim of breast screening is to reduce mortality from breast cancer by diagnosing cancer at an early stage when treatment is more successful.  In England, the NHS currently offers breast screening to women aged from 50 (first invitation by 53rd birthday) up to their 71st birthday, every 3 years.  During 2015-16, NHS England (London) re-commissioned the provision of breast screening across London. Since 1 April 2016, the model has comprised a stand-alone pan-London call/recall administration Hub (the Hub; provided by the Royal Free London NHS Foundation Trust) and 6 clinical services. Prior to this, each breast screening service in London provided an end-to-end pathway which included the functions now provided centrally by the Hub.  The Hub delivers all administration functions for London’s 6 breast screening services including scheduling, invitation, data collation, website management and a call centre for more than 1.3 million eligible clients across London.  The 6 breast screening services in London are:   * North London Breast Screening Service (Royal Free London NHS Foundation Trust) * Central & East London Breast Screening Service (Royal Free London NHS Foundation Trust) * Outer North East London Breast Screening Service (hosted by InHealth) * South West London Breast Screening Service (hosted by St Georges University Hospitals London) * South East London Breast Screening Service (hosted by Kings College Hospital NHS Foundation Trust) * West of London Breast Screening Service (hosted by Imperial College Healthcare NHS Trust)   Annually, more than 500,000 invitations are sent by the Hub and with over 350,000 managed incoming calls.  Partners Procurement Service (“PPS”) on behalf of Royal Free London NHS Foundation Trust (RFL) undertook a competitive competition through 2023/24. Ten suppliers were invited to tender for the Breast Screening Patient Communication Provision. The NHS SBS Patient/Citizen Communications & Engagement Solution Framework Lot 6, Hybrid Mail reference SBS10175 was used for this tender process.  Following contract award in January 2024, Civica Ltd commenced as the Hub’s outsourcing supplier from 01 May 2024. |

|  |
| --- |
| 2.2 Purpose |
| The purpose of this updated DPIA is to provide assurance to the trust for Civica (via Funasset Hybrid Mail interface) to continue to provide physical letter and other patient communication for London’ breast screening clients, and implement the roll out of sending correspondence to clients via email/SMS text message containing a time limited link with integrated Date of Birth validation to be able to view a PDF electronic copy of the correspondence (i.e. appointment invitation, DNA notification, normal results for 3 yearly screening routine recall).  This also continues to include appointment text message notifications 48hrs and 7 days beforehand.  In summary:   * Hybrid Mail interface will scan the top left-hand side of documents for hidden text fields (i.e. white font not visible but can still be extracted as text) containing the following details:   + Client mobile number (if available on NBSS record)   + Client email (if available on NBSS record)   + Client Date of Birth from NBSS record (DOB) * In the absence of mobile number and email address, the letter will be printed and posted to the client * In the presence of mobile number and/or email address, an email/SMS text message will be sent to the client with a link to access an electronic PDF copy of the letter * The embedded link will require the client to validate their DOB to access the letter. * The link will be time limited, such that if it is not accessed with DOB validation successfully completed within a given timeframe (i.e. 48hrs), we would revert to sending the letter via printed post format. |

|  |
| --- |
| 2.3 Scale |
| The NHSBSP is a national population screening programme.  In England, breast screening is currently offered to women aged 50 (first invitation by 53rd birthday) up to their 71st birthday.  1.3 million eligible clients within the London population invited over a 3-year screening programme period.  Annually, more than 500,000 invitations are sent by the Hub and over 350,000 managed incoming calls. |

|  |
| --- |
| 2.4 Data Flows |
| Civica Hybrid Mail service support FHIR and HL7 interfaces for direct two-way interfacing with various clinical systems. For the use case with LBSS administration Hub, the only required interface is with NBSS clinical system, using Civica’s virtual printer for capturing letter documents and an ODBC db query module for receiving SMS text data records.  The pathway for the breast screening programme consists of the following key dataflow elements for letter correspondence and text SMS reminders.  1 – Letter Correspondence   * National Breast Screening Select (BS Select) system owned by NHS digital used to identify eligible population due to 3 yearly screening. * Hub specifies batch list of eligible clients on BS Select, which in turn transfers this data onto NBSS (the national breast screening patient administration system owned by Hitachi) – point [1] of NHSBSP service spec pathway. * Hub schedule appointments and generate invitation letters on NBSS print queue (up to 6 weeks ahead of appointment date). * Hub print appointment invitation letters 4 weeks ahead of clinic date on NBSS; outsourced from NBSS to Civica via internal RFL Hybrid Mail Printer Server (RFL-BSSPrint) – refer to HybridMail dataflow flowchart below. * Hybrid Mail interface will scan letters for hidden fields of mobile number, email and DOB. As appropriate, if fields are present email/SMS text message sent to clients with PDF time limited link with DOB validation to access an electronic copy of the letter (refer to Breast Screening Electronic invites pathway diagram below) * Civica production team print and post letters to clients that do not have a mobile number/email hidden field available and clients that do not access the provided link within a given timeframe i.e. 48hrs – refer to Hybrid Mail dataflow diagram below. * The Hub will also print letters for DNA notifications, second timed appointment invitation for clients who DNA their first appointment and normal results for 3 yearly screening routine recall to clients via Civica – refer to points [2], [3] and [4] of NHSBSP screening pathway below.   2 – Text SMS Reminders  The text message data is a separate process to the letter data that is sent 4 weeks beforehand. Since the original invitation letters were issued clients will have the opportunity to rebook and cancel. As such the client lists extracted from the NBSS system for texts will vary. At a week and 48hrs before appointments, the Hub runs an NBSS report to extract text message data for upload to Civica to enable them to send reminder text messages.   * Hub extract appointment text message reminder data from NBSS and transfer to Civica via “drop box folders” on internal RFL Hybrid Mail Printer Server (RFL-BSSPrint). Refer to points [1] and [3] of NHSBSP service specification pathway. * Civica process data and send reminder text messages to clients – refer to Hybrid Mail dataflow diagram below.   Clinical communications i.e. recalls to assessment, technical recalls, diagnosis notifications are currently actioned by the individual Breast Screening services.  3 – GP outcome reports  Upon closure of screening invitation episodes, GP reports are created on NBSS. These are outsourced on a weekly basis as per the following data flow – refer to Breast Screening GP reports pathway diagram:   * Hub extract GP reports in PDF format files, 1 per breast screening service * These PDF files are then transferred to Civica via “GP report drop box folders” on internal RFL Hybrid Mail Printer Server (RFL-BSSPrint). * Civica currently process PDF data files and split these according to individual GP practices. Each GP practice is thereby sent a printed batch of GP reports. * It is proposed that GP reports are crosschecked against a GP practice code and GP email look up list held on the Hybrid Mail printer server. * GPs with an email address available on the look up list will be emailed a time limited PDF link containing the GP reports * GP practices that do not access the time limited PDF link within the email will have their reports default to be printed and sent via post * GP practice codes not on the look up list or do not have an email listed, will be sent a printed batch of GP reports via post * As the senders of the GP report emails [Civica] will be utilising a look up list with GP agreed email to send to, no validation is required, as per agreed feedback from London ICB DPOs.   Below Diagram: NHSBSP – Service Specification screening pathway (highlighted sections for patient communications generated by Hub and processed by Civica):    See below the Data flow within the Civica HybridMail system:      Below Diagram: Breast Screening GP reports (data flow of reports sent via time limited email link and alternative physical posted reports). Sender NHS.net mailbox utilised by Hybrid mail server (nbss.hybridmail@nhs.net).    Below Diagram: Breast Screening electronic letters (data flow of client appointment and normal results letters sent via time limited email PDF link with DOB validation and alternative physical posted correspondence). Sender NHS.net mailbox utilised by Hybrid mail server (nbss.hybridmail@nhs.net). |

|  |
| --- |
| 2.5 Benefits |
| Improvements in uptake and reductions in inequalities through better focused patient communication and correspondence (current Pan London average uptake approx. 65%; national standard target is 70% uptake)  Improved technology - Unified integrated system leading to improved user interface (user time and efficiency savings).  User efficiency (saving time for core jobs instead of preparing post)  Future capability for a move from ‘paper’ to ‘digital’ communication (once approved by NHSE and SQAS)  Reduced text messaging costs compared to existing provider.  Reduced letter outsourcing costs compared to existing provider.  Visibility of archived & returned mail  Royal Mail Mailmark tracking through postal network  Detailed letter Management Information (MI) reporting  Security within print centre(s)  Custom developed software  Benefits of Electronic GP reports update   * Reduced outsourcing costs * Instant access to reports sent to GPs (no wait for postal pathway)   Benefits of Electronic client appointment correspondence   * Reduced outsourcing costs, * Instant access to letters sent to clients (no wait for postal pathway), * Ability to receive correspondence in an easily accessible format with all associated inserts, maps etc that can be viewed as per client preference e.g. zoom in/out etc. |

# Section 3 – Screening Questions

|  |  |  |
| --- | --- | --- |
| Question | Response | Comments |
| Are you starting a project, programme, or research study using existing or newly collected Personal Data? *This includes Personal Data which is pseudonymised.* | Yes | Using existing data |
| Are you using Personal Data which could result in a risk of physical or emotional harm to a Data Subject in the event of a security breach or accidental disclosure? | Yes | PID for clients invited for screening |
| Are you combining Personal Data from different data sources? | Yes |  |
| Are you planning on sharing Personal Data with organisations or people who have not previously had routine access to the Personal Data? | Yes | Data shared for onward processing only by replacement supplier. |
| Are you collecting Personal Data from a source other than the Data Subject? | Yes | Already in existing systems (BS Select and NBSS) |
| Are you profiling Data Subjects or using Personal Data to decide on access to services? | No |  |
| Are you profiling children or targeting them for marketing or online services? | No |  |
| Are you tracking Data Subject’s location or behaviours? | No |  |
| Are you changing existing processes which use Personal Data? | No |  |
| Are you undertaking any type of marketing, advertising, or promoting aims or ideals? | No |  |
| Are you using Biometric Data? | No |  |
| Are you using Genetic Data? | No |  |
| Are you changing technology which Processes Personal Data, for example using a new system or supplier? | Yes | Civica Ltd – change in transmission of data to hybrid model of electronic and printed format (for non-responders to time limited link) |
| Are you implementing new technology into the Trust’s main IT infrastructure? | No |  |
| Are you implementing a new, or changes to an existing patient record system? | No |  |
| Are you starting a project, programme, or research study which will use close circuit television cameras (CCTV) or body worn video (BWV)? | No |  |
| If you answer ‘yes’ or ‘unsure’ then you must complete the full DPIA in Sections 4 to 10 | | |

# Section 4 – Data

*In this section you need to record what Personal Data fields you are using or collecting and justify why you need each field. This is to ensure you only use the minimum amount of information necessary.*

## 4.1 Personal Data – Primary data subjects

*Those who’s data is intended to be processed for the primary purpose of the DPIA*

|  |  |  |
| --- | --- | --- |
| Data Field | Tick all that apply | Justification |
| Name |  | Required as per NHSBSP Service Specification to ensure that eligible clients are invited for screening – data field on national standard letter templates |
| NHS Number |  | As above |
| Pseudonymisation number |  | As above – field from NBSS client record |
| Gender |  |  |
| Date of Birth |  | Hidden white font text field embedded within letters. These text fields will not be visible on letters when printed or viewed but will be able to be detected as electronic text within document.  Fields to enable Civica Ltd to deliver electronic correspondence/GP reports from NHS.net mailbox.  DOB validation rules to apply to client correspondence link access. |
| Physical description |  |  |
| Employment data |  |  |
| Criminal convictions |  |  |
| Financial |  |  |
| Address |  | As above |
| Home phone number |  | Required as per NHSBSP Service Specification to ensure that eligible clients are sent SMS reminder text messages for screening |
| Mobile phone number |  | Required as per NHSBSP Service Specification to ensure that eligible clients are sent SMS reminder text messages for screening and to enable Civica Ltd to send electronic correspondence link access to client email if available on NBSS records. |
| Email Address |  | Hidden white text field embedded within letters to enable Civica Ltd to send electronic correspondence link access to client email if available on NBSS records. |
| *Insert additional rows if required.* | | |

## 4.2 Special Category Personal Data – Primary data subjects

*Those who’s data is intended to be processed for the primary purpose of the DPIA*

|  |  |  |
| --- | --- | --- |
| Data Field | Tick all that apply | Justification |
| Racial or ethnic origin |  |  |
| Political opinions |  |  |
| Religious or philosophical beliefs |  |  |
| Trade union membership |  |  |
| Genetic data |  |  |
| Biometric data |  |  |
| Sex life or sexual orientation |  |  |
| Health data including occupational health |  | National NHSBSP letter and SMS text reminders templates include wording regarding invitation to breast screening appointment. |
| Mental health data |  |  |
| Health data which may be more sensitive than general health information, for example, gender reassignment or sexual health |  |  |
| *Insert additional rows if required.* | | |

## 4.3 Personal Data – Secondary data subjects

*Secondary data subjects are those who data is processed as a consequence of the DPIA’s primary purpose, for example, staff data for user accounts.*

|  |  |  |
| --- | --- | --- |
| Data Field | Tick all that apply | Justification |
| Name |  | Staff login for Hybrid Mail online interface utilise names and PC login usernames to facilitate account creation and tracking of users that printed data. |
| NHS Number |  |  |
| Pseudonymisation number |  |  |
| Gender |  |  |
| Date of Birth |  |  |
| Physical description |  |  |
| Employment data |  |  |
| Criminal convictions |  |  |
| Financial |  |  |
| Address |  |  |
| Home phone number |  |  |
| Mobile phone number |  |  |
| Email |  | Staff login for Hybrid Mail online interface utilise staff NHS.net email for password resets |
| *Insert additional rows if required.* | | |

## 4.4 Special Category Personal Data – Secondary data subjects

*Secondary data subjects are those who data is processed as a consequence of the DPIA’s primary purpose, for example, staff data for user accounts*

|  |  |  |
| --- | --- | --- |
| Data Field | Tick all that apply | Justification |
| Racial or ethnic origin |  |  |
| Political opinions |  |  |
| Religious or philosophical beliefs |  |  |
| Trade union membership |  |  |
| Genetic data |  |  |
| Biometric data |  |  |
| Sex life or sexual orientation |  |  |
| Health data including occupational health |  |  |
| Mental health data |  |  |
| Health data which may be more sensitive than general health information, for example, gender reassignment or sexual health |  |  |
| *Insert additional rows if required.* | | |

# Section 5 – Legal

|  |
| --- |
| 5.1 Lawfulness, fairness & transparency  Processed lawfully, fairly and in a transparent manner in relation to the data subject |
| See section 5.2, 5.3 and 5.4 for lawfulness.  Fairness is assessed throughout this document.  See section 8.1 for Transparency. |

|  |
| --- |
| 5.2 Purpose Limitation  Personal Data is collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. |
| To invite eligible client cohort for Breast Screening appointments as per NHSBSP Service Specification, including letters for DNA’s and routine outcome for return to 3 yearly screening.  Date of Birth, Mobile Number and Email address client details are added to letters as embedded hidden fields to solely facilitate the sending of electronic correspondence links to clients.  Clinical communications i.e. recalls to assessment, technical recalls, diagnosis notifications are currently actioned by the individual Breast Screening services. |

|  |
| --- |
| 5.3 Data Minimisation  Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed |
| See section 4.1 and 4.2 for data minimisation. |

|  |
| --- |
| 5.4 Accuracy  Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay |
| The personal data used in Breast Screening client communications originates from Primary Care providers (GPs) and the national spine via the national BS Select system, which then in turn feeds to client NBSS records.  As such the data is maintained and accurate as per what is provided by Primary Care Providers (GPs).  GP reports are allocated according to the GP practice to which each individual client is registered on their NBSS record.  Emails used to send GP reports via PDF link are GP agreed NHS.net emails provided by London ICB Primary Care Teams.  As per feedback from GPs, the email look up list will be updated as appropriate.  Client mobile numbers, DOB and email addresses used to facilitate electronic invite messages will originate from Primary Care providers (GPs) and the national spine via the national BS Select system, which then in turn feeds to client NBSS records. |

|  |
| --- |
| 5.5 Storage Limitation  Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary; |
| See section 7.5 for details on retention. |

|  |
| --- |
| 5.6 Integrity and Confidentiality  Personal Data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. |
| See section 5.4 for confidentiality.  See section 6 for integrity. |

|  |
| --- |
| 5.7 Accountability  The Controller shall be responsible for, and be able to demonstrate compliance with, the data protection principles |
| Accountability is demonstrated throughout this document. |

***\*\*\*\*Information Governance Directorate use only\*\*\*\****

|  |
| --- |
| 5.8 Personal Data Lawful basis (UK GDPR Article 6) |
| Under UK GDPR, for processing personal data in the delivery of direct care, and for providers’ administrative purposes, the most appropriate Article 6 condition that is available to all public funded health and social care organisations is:  Article 6(1)(e) “the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”  DPA Section 8 Condition. The lawfulness of processing personal data set out in Article 6(1) (e) of the UK GDPR (as above) is permitted under Section 8 (d) of DPA 2018: Processing is necessary for the exercise of statutory functions.  *This section is for completion by the Information Governance Directorate.* |
| *If the Article 6 lawful basis contains the word ‘necessary’ that necessity must be demonstrated below.*  *If the lawful basis contains the words ‘legitimate interests’, the legitimate interests test must be demonstrated below.*  *If the lawful basis contains the word ‘consent’ the consent process must be documented below.* |
| The processing is necessary for sending client communications in connection to the operation of the NHSBSP in London.  *This section is for completion by the Information Governance Directorate.* |

***\*\*\*\*Information Governance Directorate use only\*\*\*\****

|  |
| --- |
| 5.9 Special Category Data Lawful Basis (UK GDPR Article 9) |
| In addition to the above, an Article 9 condition of processing must also be used;-  UK GDPR Article 9(2)(h) “…processing is necessary for the purposes of preventive or occupational medicine, for…the provision of health or social care or treatment or the management of health or social care systems and services…”  For the purposes of Article 9(2) (h) of the UK GDPR, the circumstances in which the sharing/processing of special categories of personal data is carried out is subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR (obligation of professional secrecy), which include circumstances in which it is carried out under DPA Section 11(1) supplementary:   * by or under the responsibility of a health professional, or * by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law   The terms “health professional” and “social work professional” are defined in Section 204 of DPA 2018, and include a broad range of different professionals.  When relying on condition (h), you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.  Health or social care purposes  2 (1) This condition is met if the processing is necessary for health or social care purposes.  (2) In this paragraph “health or social care purposes” means the purposes of—  (d) the provision of health care or treatment,  *This section is for completion by the Information Governance Directorate.* |
| *If the lawful basis contains the word ‘necessary’ that necessity must be demonstrated below.*  *If the lawful basis contains the words ‘legitimate interests’, the legitimate interests test must be demonstrated below.*  *If the lawful basis contains the word ‘consent’ the consent process must be documented below.* |
| The processing is necessary for sending client communications in connection to the operation of the NHSBSP in London.  *This section is for completion by the Information Governance Directorate.* |

|  |
| --- |
| 5.10 Duty of Confidentiality |
| The NHSBSP operates on the principle of implied consent for invitation screening when a client is registered with a GP and meets the eligibility criteria for the screening programme i.e. 50-70 years old.  Eligible clients are invited for breast screening every 36 months.  Clients who choose to permanently opt out (ceased) from the programme (informed subject choice), and those who are no longer eligible due to medical reasons (bilateral mastectomy or Mental Capacity Act (MCA)), can be permanently opted out (ceased) from the NHSBSP call and recall process.  A client who is permanently opted out (cease) from NHSBSP will not receive any invitation or reminder letters from the Hub unless she chooses to opt back into the programme.  Clients who have previously opted out of the NHSBSP will no longer be contacted.  Clients who have not previously opted out will receive initial communication prior to opt out.  NHSBSP Ceasing Guidance - <https://www.gov.uk/government/publications/opting-out-of-breast-screening/guidance-on-opting-out-cease-from-breast-screening> |

|  |
| --- |
| 5.11 Trust Ethical Approval  Complete when conducting research only |
| N/A, this is not research. |

|  |
| --- |
| 5.12 Health Research Authority (HRA) Approval  Complete when conducting research only |
| N/A, this is not research. |

|  |
| --- |
| 5.13 Confidentially Advisory Group (CAG) Approval  Secondary use of Identifiable health data without consent only |
| N/A, this is not a secondary use. |

# Section 6 – Technical and Organisational Controls

|  |
| --- |
| 6.1 Access Controls |
| NBSS access for generating and printing letters is controlled under the following RFL Trust and NBSS policies:   * RFL Information Security Policy * RFL Confidentiality Policy * NHS Cancer Screening Programmes System Level Security Policy for the NBSS system     RFH IT limits the availability of NBSS shortcuts such that these are only mapped specifically to Breast Screening Service workstations. NBSS access requires that you are logged into the Trust network or VPN e.g. Citrix remote connection.  Hub access controls to NBSS, are effectively managed due to an established starters and leavers process via designated NBSS System Manager users. System Manager NBSS user accounts are restricted to the following members of the Hub Management Team:   * Assistant Operations Manager * Service Managers * Office Managers * Team Leaders   As part of induction and leavers checklists that are completed by staff line managers, arrangements are made to create/activate and disable/deactivate NBSS accounts of new staff and leavers, respectively. In addition, NBSS automatically disables accounted not accessed for a prolonged period with login inhibited and password reset via a System Manager user required.  For the Hub to access the Online Web Mail portal, the user must be logged into the RF Trust Network or VPN as only whitelisted IPs are permitted to access the website interface. The RF outbound IP has been added to the Hybrid Mail online portal Whitelist and so Hub users are able to access the portal from the Trust network.  Access to the Hybrid Mail service is controlled by clients Active Directory authentication (SAML) providing user level of access controlled by users group memberships within clients AD.  Within Royal Free AD (Azure AD application) specific Hybrid Mail groups will be created for each access level. With Royal Free IT or service managers ensuring the correct user group membership is maintained for its users of the service. Including creation and removal of accounts and group memberships for starters/leavers, managed within Royal Free AD.  Solution provided three levels of role-based access, User, Manager and Admin. Allocated based on user group membership, these group memberships are controlled from AD.   * User - Provides Web portal access to just view their Mail Menu, allowing a user to only view documents their have submitted, showing Queued, Printed and Returned/Rejected items. User is able to View and delete just their own items. * Manager - Provides Web portal access to view their submitted documents and those of users within their group, allowing manager to View and delete any items submitted within their group. * Admin - Provides Web portal access to Mail and Admin Menu, allowing an admin to upload and remove letter attachments, create/modify input template profiles, use Find Mail function to search system for specific letter documents, to run and schedule MI reports on system.   NBSS requires that passwords are regularly changed and updated on an 8-weekly basis.  Civica web portal utilises Azure AD single Sign-on (SSO) authentication to manage user accounts.  SSO authentication has been in place since late 2024. |

|  |
| --- |
| 6.2 Physical Controls |
| The RF components are located in secure server rooms at Hampstead and Chase Farm; covered by Trust information security policies.  Civica production controls  The RF components are located in secure server rooms at Hampstead and Chase Farm; covered by Trust information security policies.  Civica hosted environment  Our Managed Print Service hosting platforms is audited and recertified to ISO27001 hosted on co-location infrastructure in Tier 4 class datacentre, Location Exeter UK  Access to physical server environment at Exeter data centre uses three-tiered access, with only authorised DC staff allowed access to server room & cabinets. Data centre customers Funasset have escorted access to data centre build / workshop rooms only, and not allowed access into server rooms. Physical security includes CCTV surveillance, 24-hourmonitored alarms, and ISO 27001-compliant secure storage area.  Remote access to server environment is the responsibility of Funasset Technical Director allocating and authorising user access rights in conformity with ISMS policies, on a need basis, staff access accounts are unique (not shared) and use 2FA. Access to any client hosted systems can only be gained from within Funasset internal network LAN, staff have Cisco VPN access to Funasset network, with 2FA using Cisco mobile authenticator app. Once authenticated to internal LAN, allowed user accounts can gain RDP access to specific client servers. Client servers are isolated on dedicated VLANs with Cisco network switching management to further control limit network access. |

|  |
| --- |
| 6.3 Technical Controls |
| The RF hosted component is logically segregated and connections outbound are controlled by a default block with explicit pass list. A single rule permits access from the internal print server to the Civica system via the public internet. Data is encrypted in flight using at least TLS 1.2.  Electronic Delivery of GP reports and Client Correspondence:  An NHS.net email exists for the Hybrid Mail platform ([nbss.hybridmail@nhs.net](mailto:nbss.hybridmail@nhs.net)).  The mailbox would have restricted access to the Hybrid Mail platform that would use the secure NHS.net mailbox exchange to facilitate the delivery of the following items:   * GP reports to GP practice NHS.net email mailboxes in the form of a time limited PDF link within the emails, * Client appointment and normal result correspondence containing demographic details (non-sensitive health information) in the form of time limited and Date of Birth validated PDF links within the emails.   Civica hosted services:  Defined in our GDPR Policy and ISMS system, appropriate technical and organisational measures are implemented in order to provide data security. These measures safeguard personal data from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. These measures relate to the security of data which merit protection, whether processed electronically or in paper form.  These technical and organisational measures form part of an Information Security Management System (ISMS) certified to ISO27001 and are constantly revised in accordance with technological developments and organisational changes.  Funasset is committed to industry best practices concerning security measures which look to prevent the loss, misuse and alteration of the information in our possession. We use various audited and certified security measures to protect the information we collect (as appropriate to the classification), including encryption, firewalls and access controls.  Perimeter Defence is provided by Sophos XGS next-gen firewalls, providing Deep Packet Inspection, Zero-Day and ML Protection, Active Threat Protection, DDoS protection against today’s most sophisticated DDoS attacks, TLS 1.3 Decryption.  Webroot end point pretention for AV and Malware defences.  Solution has pen tests run annually by 3rd party, in addition we use Qualys external and internal network agents to scan our services on a weekly basis. Any issues found with severity 5- 3 being actioned and resolved immediately.  Data transit is protected by https TLS1.2 SSL 256b encryption with our hosted webservice for all data transfers between client and SPS.  Data at rest storage is encryption to standards, AES-256 certified to FIPS 140-2 Level 2. |

|  |
| --- |
| 6.4 Training |
| Royal Free staff complete training to deliver as per roles and systems (NBSS, BS Select) in line with NHSBSP guidelines and Trust policies (as outlined in section 6.1)  All staff, processes and facilities are subject to regular audits via ISO9001 or ISO27001 internal audits and the six monthly independent ISO audits. There are six monthly physical security audits carried out by the UK physical security manager. In addition, Funasset IT risk assessments are completed annually. Staff are provided with training in the operational processes prior to working on any systems or equipment and are provided with operational guidelines, these are regularly updated as the system matures. Training including information security awareness is provided for all new staff, staff moving to the contract and annually thereafter which ensures staff are aware of the specific security requirements and latest procedures they must adhere to at all times. These procedures are subject to regular updates and are written in line with Funasset policies, ISO controls and customer specific requirements. |

|  |
| --- |
| 6.5 Anonymisation Process  Complete when Anonymising Personal Data only |
| N/A |

|  |
| --- |
| 6.6 Pseudonymisation Process  Complete when using Pseudonymised Personal Data only |
| N/A |

|  |
| --- |
| 6.7 Audit |
| Access to the NBSS is audited. User access is controlled by designated users with System Manager access. Leavers have access revoked from the NBSS.  For granular auditing, NBSS SPRPT audit by SX number reports and System Manager security level audits are possible.  All activity on the NBSS system is recorded and is able to be picked up in the above audit processes.  Hub and Clinical Service’s complete daily basis monitoring of the NBSS SMSTA (print queue) and SIL (print reports) functions to review unprinted letter in the print queue and cross reference processing reports from outsourcing provider to confirm letters that have been printed and processed. |

|  |
| --- |
| 6.8 DCB0129  For completion when developing and maintaining Health IT Systems for use within the health and care environment |
| DCB 0129 completed for sub-processor managing the appointment letters and SMS messages.  Clinical Risk Management Plan: Hybrid Mail    Clinical Safety Case Report: Hybrid Mail    Funasset\_Integrated\_Mail\_hazard log\_v1.1 |

|  |
| --- |
| 6.9 DCB0160  For completion when deploying, using, maintaining, or decommissioning Health IT Systems within the health and care environment. |
| In progress, please see Section 12 – Actions |

|  |
| --- |
| 6.10 Digital Technology Assessment Criteria (DTAC)  For completion when deploying Health IT Systems within the health and care environment |
| DTAC completed for sub-processor managing the appointment letters and SMS messages. |

|  |
| --- |
| 6.11 Decommissioning  For completion when deploying Health IT Systems within the health and care environment |
| Following the end of the contract, Civica will delete RFL data from their systems and to return and return any copies requested in an agreed format to the trust.  Once RFL confirms successful receipt of this and instructs the Civica to do so, the Civica will irretrievably destroy all RFL data using an agreed methodology. |

# Section 7 – Process and Policy

|  |
| --- |
| 7.1 Policy |
| Policy frameworks for NBSS controlled access as per the NHS Cancer Screening Programmes System Level Security Policy for the NBSS system    NBSS use for generating and printing letters covered by the following policies:   * RF Information Security Policy * RF Confidentiality Policy     The Hub’s SOP covering the processes of printing letters to the current provider are attached below:    *Name any supporting policies or procedures used to support the processing, for example, Information Governance Policy, Working from Home Policy, Starters and Leavers Process.* |

|  |
| --- |
| 7.2 Incident Reporting |
| Use of existing RFL Trust incident reporting processes (DATIX) and SQAS (Screening Quality Assurance) SIAF (Screening Incident Assessment Submission) submissions for serious incidents.  Example SQAS SIAF form attached below:    As outlined in the attached Civica GDPR compliance policy attached    Civica deploys a robust security incident reporting process, which operates as follows:   * The Incident reported to Manager. * The Manager reports details of the incident to the Information Security Officer. * A Report is created recording:   + Unique ID   + Date   + Time   + Reported by   + Reported to   + Owner   + Details of incident   + Root cause   + Actions to remediate   + Status open/closed * Concerned parties are informed including any affected customers. * If required Civica corporate response team are informed. * Actions to remediate are discussed with relevant parties. * Actions are completed. * Incident is closed. * Repeat incidents are reviewed for suitability of further controls. * Issues are discussed at quarterly management review meetings.   As per the agree approved supplier contract between RFH Trust and Civica, the agreed timeframe is within 24hrs for Civica to inform the Hub to ensure that the RFH Trust is rapidly aware on discovery of a serious incident. |

|  |
| --- |
| 7.3 Business continuity planning (BCP) |
| System runs on the Royal Free site on the VxBlock virtual infrastructure, is backed up nightly, and has a DR replica in Chase Farm. Recovery time objective is 48 hours, recovery point is 24 hours.  For Hub users  In the event that the letter and SMS outsourcing systems become unavailable, this will look to be declared to regional NHSE commissioners and SQAS as a potential incident.  Hub Senior Management Team would convene emergency meetings and liaise with relevant parties and stakeholders i.e. Breast Screening Service, Civica etc, to agree next steps to have the matter resolved. The Hub Business Continuity Plan would be discussed and appropriate steps implemented.  For Civica Hosted environment  We run both Primary and DR datacentres providing service resilience, with identical infrastructure and VMware clusters at both locations. Veeam Backup & Replication software is used to manage VM backups to local NAS storage within Primary data centre. Restoring from backup takes under 1 hour, for VM replications held at DR location these power up within 5 mins of initiating failover. All Veeam backups are encrypted, holding six restore points for all live VMs, NAS storage.  No data backups are held outside of secure datacentre network environment, physical backup media is not used/permitted.  Hosted service has access to duplicate print fulfilment centres, if there is a disaster recovery scenario, work can be immediately switched to an alternative fulfilment centre. The Civica Mail servers are hosted within a resilient Tier 4 Data Centre the most stringent level of which is designed to host mission critical computer systems with fully redundant subsystems and compartmentalised security zones controlled by biometric access controls methods. |

|  |
| --- |
| 7.4 Records Management |
| Records are digitally held in the NBSS system.  PID only for purpose of inviting for screening. PID managed according to NHSBSP guidelines.  Link to NHSBSP guidance: <https://www.gov.uk/government/publications/breast-screening-manage-mammograms-and-records/retention-storage-and-disposal-of-mammograms-and-screening-records> |

|  |
| --- |
| 7.5 Retention |
| Source data is retained according to NHSBSP guidelines.  Link to NHSBSP guidance: <https://www.gov.uk/government/publications/breast-screening-manage-mammograms-and-records/retention-storage-and-disposal-of-mammograms-and-screening-records>  Letters are generated by the NBSS system and sent to Civica; local NBSS copy held on print queue retention period of 6 months.  Civica Hybrid Mail Hybrid Mail systems run a data retention period of 30 days, primarily for the need to manage any Royal Mail returned letters, allowing Web portal users to view PDF of letters retuned by Royal Mail. |

|  |
| --- |
| 7.6 Lifecycle/end of life |
| Civica Mail Software runs automated tasks every 24 hours to delete data and db. records associated with client data held, based on configured retention period.  Upon request a clients data retention can be adjusted or reduced to zero for the removal of all data records held.  Upon Subject Access Request, an individual’s record can be removed from the system if processed within last 30 days and still held on system. |

# Section 8 – Data Subject Rights

|  |
| --- |
| 8.1 The right to be informed |
| This is fulfilled through the Royal Free London patient facing Privacy Notice: <https://www.royalfree.nhs.uk/patients-visitors/privacy-notice/> The Privacy Notice explains how their information will be used and who it may be shared with. |

|  |
| --- |
| 8.2 The right of access |
| Patients can exercise this right by following the process in the trust’s patient facing privacy notice [Privacy notice | For patients, carers and visitors | The Royal Free](https://www.royalfree.nhs.uk/patients-visitors/privacy-notice/) Data subjects are able to request information the trust holds on them via the established SAR process.  Covered by RF Trust subject access policies    Letter templates printed from NBSS attached below:    Opting out ceasing policy as per NHSBSP guidance: <https://www.gov.uk/government/publications/opting-out-of-breast-screening/guidance-on-opting-out-cease-from-breast-screening> |

|  |
| --- |
| 8.3 The right to rectification |
| Patients can exercise this right by following the process in the trust’s patient facing privacy notice [Privacy notice | For patients, carers and visitors | The Royal Free](https://www.royalfree.nhs.uk/patients-visitors/privacy-notice/)  As outlined in section 5.4, the personal data used in Breast Screening client communications originates from Primary Care providers (GPs) and the national spine.  Data Subjects can have inaccurate information that we are processing corrected by notifying their GP practice to make corrections to their Primary Care Record and this will in turn feed into BS Select and NBSS.  The Hub process is not to change any NBSS record unless the change is reflected on BS Select and as per above direct clients who contact us to their GPs.  The breast screening services do have the option to update NBSS for a short-term period i.e. address correction whilst the client visits their GP to have their record updated to ensure that the result letter is directed to the most up to date address. But ultimately when a feed comes down from BS Select to NBSS, this correct will be reversed until the primary care record is updated. |

|  |
| --- |
| 8.4 The right to erasure |
| Patients can exercise this right by following the process in the trust’s patient facing privacy notice [Privacy notice | For patients, carers and visitors | The Royal Free](https://www.royalfree.nhs.uk/patients-visitors/privacy-notice/)  As per NHSBSP guidance, this would require ad hoc engagement with the national NHSBSP team, NHS Digital (owner of BS Select), Primary Care and Hitachi (owner of the NBSS). |

|  |
| --- |
| 8.5 The right to restrict processing |
| Patients can exercise this right by following the process in the trust’s patient facing privacy notice [Privacy notice | For patients, carers and visitors | The Royal Free](https://www.royalfree.nhs.uk/patients-visitors/privacy-notice/)  As per section 5.10, a client who is permanently opted out (ceased) from NHSBSP will not receive any invitation or reminder letters from the Hub unless she chooses to opt back into the programme.  Clients who have previously opted out of the NHSBSP will no longer be contacted.  Clients who have not previously opted out will receive initial communication prior to opt out.  NHSBSP Ceasing Guidance - <https://www.gov.uk/government/publications/opting-out-of-breast-screening/guidance-on-opting-out-cease-from-breast-screening> |

|  |
| --- |
| 8.6 The right to data portability |
| The right to data portability does not apply in this circumstance. Consent is not the legal basis for processing and neither is the processing by automated means |

|  |
| --- |
| 8.7 The right to object |
| Patients can exercise this right by following the process in the trust’s patient facing privacy notice [Privacy notice | For patients, carers and visitors | The Royal Free](https://www.royalfree.nhs.uk/patients-visitors/privacy-notice/)  As per section 5.10, a client who is permanently opted out (ceased) from NHSBSP will not receive any invitation or reminder letters from the Hub unless she chooses to opt back into the programme.  Clients who have previously opted out of the NHSBSP will no longer be contacted.  Clients who have not previously opted out will receive initial communication prior to opt out.  NHSBSP Ceasing Guidance - <https://www.gov.uk/government/publications/opting-out-of-breast-screening/guidance-on-opting-out-cease-from-breast-screening> |

|  |
| --- |
| 8.8 Rights in relation to automated decision making and profiling. |
| N/A, this process does not involve any automated decision making or profiling. |

# Section 9 – Supporting Documents

|  |
| --- |
| 9.1 Supporting documents |
|  |

# Section 10 – Consultation

|  |
| --- |
| 10.1 Consultation |
| Partners Procurement Service (“PPS”) on behalf of Royal Free London NHS Foundation Trust (RFL) undertook a competitive competition through 2023/24. Ten suppliers were invited to tender for the Breast Screening Patient Communication Provision.  The NHS SBS Patient/ Citizen Communications & Engagement Solution Framework Lot 6, Hybrid Mail reference SBS10175 was used for this tender process.  The framework agreement currently in use (currently held by Synertec Ltd) was due to expire in March 2022. The contract is historic and has continued to be renewed annually by short term extensions for a number of years.  A mini competition was undertaken, under the NHS SBS Patient/Citizen Communications and Engagement Solution Framework, which provides a suitable mix of suppliers for the required service.  Contract awarded to CIVICA, as per RFL procurement led competitive tender process.  The above change in Hub outsourcing provider has had the following stakeholders consulted as part of the tender process:   * NHSE (London Region) Commissioning Team * SQAS Regional Team * London Breast Screening Improvement Board   The key aims of this project are to review how the London Breast Screening Hub can ensure that it provides London’s eligible breast screening population with the best possible service in relation to patient correspondence. Whilst continuing to serve the needs of London’s six breast screening services hosted by five different NHS & private organisations; ensuring that NHSE and the RFL receive the best possible contractual value.  The preferred supplier should be able to deliver patient communications in various formats, text reminders, self-service portal for requests and extensive provider support. |

**Move to next section.**

# Section 11 – Risks

# Risk Matrix

Multiplying the likelihood score for the potential adverse outcome of the risk by the adverse consequence that might arise results in the risk score.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood ð** | **1 Rare** | **2 Unlikely** | **3 Possible** | **4 Likely** | **5 Almost certain** |
| **Consequenceò** |  |  |  |  |  |
| **5 Catastrophic** | **5** | **10** | **15** | **20** | **25** |
| **4 Major** | **4** | **8** | **12** | **16** | **20** |
| **3 Moderate** | **3** | **6** | **9** | **12** | **15** |
| **2 Minor** | **2** | **4** | **6** | **8** | **10** |
| **1 Negligible** | **1** | **2** | **3** | **4** | **5** |

For grading risk, the scores obtained from the risk matrix are assigned grades:

|  |  |
| --- | --- |
| 1 - 3 | Low risk |
| 4 - 6 | Moderate risk |
| 8 - 12 | High risk |
| 15 - 25 | Extreme risk |

**Any risks requiring ongoing mitigation must be incorporated into project plans and/or local risk management processes.**

*Complete the table below with the identified risks and controls which have been implemented.*

| ID | Description | Consequence | Initial Score (probability x severity) | Controls | Controlled score (probability x severity) | Status |
| --- | --- | --- | --- | --- | --- | --- |
| 01 | Confidential information is available to unauthorised persons.  System is compromised and becomes unavailable.  Patient may be unintentionally exposed to clinically sensitive information | Inappropriate access to Personal Data, loss of patient confidence, regulatory action, , breach of UK GDPR, Caldicott Principles and common law duty of confidentiality | 4 x 3 = 12 | User access are supported by appropriate security controls.  User account management is maintained by administrated access levels for staff with differing roles. (e.g. assigning RBAC)  For attempts at unauthorised access:  - System security controls are ISO 27001 certified [Ref 4]  - PEN tests are conducted on a regular basis | 1 x 3 = 3 | Accepted |
| 02 | Malicious third-party acquiring control of target IP | Inappropriate access to Personal Data, loss of patient confidence, regulatory action | 3 x 3 = 9 | Implementation certificate swap controls via SSO implementation. | 1 x 3 = 3 | Accepted see Section 12 - Actions |
| 03 | Leavers having access to their login and patient information until license reassigned | Inappropriate access to Personal Data | 3 x 3 = 9 | User management process linked to trust starters and leavers process and linked to ADFS SSO. | 1 x 3 = 3 | Accepted |
| 04 | There is a risk that personal data is retained for longer than the intended purposes, contrary to data protection law. | Results in a greater risk to the rights and freedoms of individuals in the event of system compromise or personal data breach. | 3 x 4 = 12 | The Processor is contractually committed to destroying or returning data at the request of the Controller. | 1 x 4 = 4 | Accepted |
| 05 | Risk that anyone with access to the mobile SMS is sent to will see sensitive medical information from SMS message | Inappropriate access to Personal data, breach of UK GDPR. | 4 x 4 = 12 | Patient will need to authenticate that they are the correct recipient of the SMS reminder | 1 x 4 = 4 | Accepted |

*Controlled risks score acceptance thresholds:*

* *1 – 6 can be accepted by the Information Asset Owner*
* *7 – 12 can only be accepted by the Senior Information Risk Owner or Group Executive Committee*
* *13 and above can only be accepted by the Group Executive Committee or Trust board*

# Section 12 – Actions

*Complete any outstanding actions which need to be completed. These are likely to be controls not yet fully implemented.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Action Owner | Action Description | Due Date | Date Completed | Status |
| 01 | Kenneth Blake – Asst Operations Manager (on behalf of Royal Free London Admin Hub) | Engage with RFL Clinical Safety Officer to undertake DCB0160 assessment. | 30/06/2024 | 15/05/2024 | Completed |
| 02 | Claire McCafferty – Business Development Manager (on behalf of Civica)  &  Mark Dawson – Managing Director (behalf of Funasset) | Review password compliance to update in line with Trust Password Protection policy. | 30/06/2024 | 19/04/2024 | Completed |
| 03 | Claire McCafferty – Business Development Manager (on behalf of Civica)  &  Mark Dawson – Managing Director (behalf of Funasset) | Implement Azure AD Single Sign On (SSO) authentication. | 30/06/2024 | 31/10/2024 | Completed |
| *Insert additional rows if required, delete unused rows.* | | | | | |

# Section 13 – Review and Approval

|  |  |
| --- | --- |
| 13.1 Information Asset Owner | |
| Comments | None |
| Approval | Approved |
| Name | Julia Kitteringham |
| Signature | By email |
| Date | 16/04/2025 |

|  |  |
| --- | --- |
| 13.2 Caldicott Guardian | |
| Comments | None |
| Approval | Approved |
| Name | Kilian Hynes |
| Signature | By email |
| Date | 23/04/2024 |

|  |  |
| --- | --- |
| 13.3 Data Protection Officer | |
| Comments | N/A |
| Approval | Approved |
| Name | Kevin Winter |
| Signature | By email |
| Date | 22/04/2024 |

|  |  |
| --- | --- |
| 13.4 Senior Information Risk Owner | |
| Comments | None |
| Approval | Approved |
| Name | Emma Kearney |
| Signature | By email |
| Date | 23/04/2024 |

# Annex 1 – Definitions

|  |  |  |
| --- | --- | --- |
| **Term** | **Abbreviation** | **Description** |
| ‘Anonymous' or 'Anonymised' |  | Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. |
| ‘Caldicott Guardian' | CG | A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people’s health and care information and making sure it is used properly. |
| ‘Common Law Duty of Confidentiality ' | CLDoC | Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges. It is an offence to breach common law. |
| ‘Confidential Information' |  | Information whether spoken or written. Also see 'Information', and 'Confidentiality' |
| ‘Confidentiality' |  | The concept of spoken or written information being handled in strict privacy or secrecy. |
| ‘Controller' |  | ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| ‘Corporate Records' |  | Information generated and received by a Trust other than clinical/care (or service user) information. The term describes the records generated by a Trust’s business activities, and therefore include:  • Policies and processes • Lists and registers • Business plans and business cases • Minutes of meetings • Estates/Engineering;  • Financial;  • Information Management & Technology; • Personnel/Human Resources; • Contracts and supplies. |
| ‘Data' |  | Data is an individual unit that contains raw materials which do not carry any specific meaning. Also see 'Information' |
| ‘Data Protection Act 2018' | DPA 18 | The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK’s status outside the EU. It sits alongside and supplements the UK GDPR - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner’s functions and powers. |
| ‘Data Protection Legislation' |  | The term used to describe all data protection legislation including, Data Protection Act 2018 (DPA 2018) and United Kingdom General Data Protection Regulation (UKGDPR) as referenced in the DPA 2018, The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) (as amended) and all applicable laws and regulations relating to the Processing of the personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any other national Supervisory Authority. |
| ‘Data Protection Impact Assessment' | DPIA | A process to systematically identify and minimise data protection risks. A requirement by law. |
| ‘Data Security and Protection Toolkit' | DSPT | An online self-assessment that allows organisations with access to NHS data to measure their performance against the National Data Guardian’s 10 data security standards. It is both a legal and contractual requirement to complete the assessment. |
| ‘Data Subject' |  | A natural person about whom a Controller holds personal data and who can be identified, directly or indirectly, by reference to that personal data. |
| ‘Information' |  | Information is a group of data that collectively carries a logical meaning. Information depends on data. Also see ‘Data’ |
| ‘Information Asset' | IA | An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles. |
| ‘Information Asset Administrator' | IAA | IAAs ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date. These roles are filled for example, by an operational member of staff who is responsible for one or more information assets. |
| ‘Information Asset Owner' | IAO | Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the Trust. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. They are accountable for information assets. |
| ‘Information Commissioner' |  | The Information Commissioner is a "corporation sole" with the powers, authority, duties and responsibilities of the role vested in one person and passing from one holder of that role to another. The Information Commissioner enforces and oversees the Data Protection Act 2018, UK GDPR, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Privacy and Electronic Communications Regulations. |
| ‘Information Commissioner's Office' | ICO | The Information Commissioner's Office (ICO), which supports the Information Commissioner in their work, is a non-departmental public body sponsored by the Department for Digital, Culture Media and Sport. Although the Commissioner operates independently in the exercise of their statutory functions, some issues require the approval of the Secretary of State such as funding and the level of notification fees. |
| ‘Information Governance' | IG | Information governance (IG) is a term used to describe how information is used, both personal data and corporate information. It covers system and process management, records management, data quality, data protection and the controls needed to ensure information sharing is secure, confidential and responsive. |
| ‘Information Governance Group' | IGG | The Trust's internal group responsible for Information Governance oversight. |
| ‘Information Incident' |  | An incident involving information or data. Also see 'Personal Data Breach', 'Data' and 'Information' |
| ‘Information Risk' |  | A risk what relates to the use, or security of data or information. Also see 'Data' and 'Information' |
| ‘Must' |  | References something that must happen. There is not scope to deviate. |
| ‘Personal Data' |  | ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| ‘Personal Data Breach' |  | ‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; |
| ‘Privacy' |  | The state of being free from public scrutiny or from having secrets or personal information shared. |
| ‘Privacy Notice' | PN | A public statement published on the Trust website telling data subjects, regulators and other stakeholders what the Trust does with personal information. |
| ‘Process' |  | See 'Processing' |
| ‘Processed' |  | See 'Processing' |
| ‘Processing' |  | ‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| ‘Processor' |  | ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| ‘Pseudonymisation' or 'Pseudonymised' |  | The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.” |
| ‘Records Management' |  | The term used to describe how records are stored, used, and destroyed. |
| ‘Senior Information Risk Owner' | SIRO | The role of the SIRO is to take ownership of the Trust information risk, act as an advocate for information risk on the Board and provide written advice to the Trust Chief Executive on the content of their annual governance statement in regard to information risk. |
| ‘Should' |  | References something that should happen useless there are exceptional circumstances which can be demonstrated. |
| ‘Supervisory Authority' |  | The relevant supervisory authority in the territory where the parties processing personal data are established. Also see 'Information Commissioner's Office' |
| ‘United Kingdom General Data Protection Regulations' | UK GDPR | UK GDPR sits alongside the DPA 2018 and is the main data protection law in the UK |