Data Protection Impact Assessment (DPIA) for Healthtech-1

|  |  |
| --- | --- |
| **Approved by** | Aaron Cameron |
| **Date approved** | 11th September 2023 |
| **Name and title of originator/author** | Assistant Practice Manager  |
| **Description** | Healthtech-1 New Patient Registration Automation |

Version Control

|  |  |
| --- | --- |
| **Version number** | Healthtech-1 v1.4Health Organisation v.1.0 |
| **Supersedes** | N/A - this is the first |

Monitoring

|  |  |
| --- | --- |
| **Monitoring method** | e.g. Reviewed by Practice Manager or IG lead |
| **Frequency** | Annually  |

Document Review Control Information

| **Version** | **Date** | **Reviewer Name(s) and Job title** | **Change/amendment**  |
| --- | --- | --- | --- |
| 1.0 | 11.09.2023 | Assistant Practice manager | New document  |
|  |  |  |  |
|  |  |  |  |

**Contents**

[**1. What is a DPIA and what should it include? 4**](#_heading=h.hh9c2keu7vok)

[**2. Key Details 5**](#_heading=h.x1eg4fag62dk)

[**3. Controllers and Processors 10**](#_heading=h.4d34og8)

[**4. Personal data 13**](#_heading=h.2s8eyo1)

[**4. Access and reporting 31**](#_heading=h.17dp8vu)

[**5. Business continuity planning 36**](#_heading=h.3rdcrjn)

[**6. Direct marketing 36**](#_heading=h.26in1rg)

[**7. Automated processing 37**](#_heading=h.lnxbz9)

[**8. Risk Management and action plan 38**](#_heading=h.35nkun2)

[**9. Reviewed By**](#_heading=h.3egnd66li26)

 [**44**](#_heading=h.3egnd66li26)

[**Appendix A: Definitions and Glossary 45**](#_heading=h.u12ah8q4ccud)

[**Appendix B: Data points stored and used to match patients to the clinical record. 47**](#_heading=h.z4zlcnh8bjf)

[**Appendix C: Full list of data points collected and stored from the patient registration forms 48**](#_heading=h.j50rdygobprc)

[**Appendix D: Full list of data points collected and stored by customer.io (EU), Twilio and Postmark 51**](#_heading=h.hbhqy5mt96k2)

[**Appendix E: List of variables and the questions on the form. 53**](#_heading=h.v18c2s9m7x1m)

[**Appendix F: System Requirements 58**](#_heading=h.4z0feeyc2d1t)

[**Appendix G: Automation Smartcard RBAC Positions 59**](#_heading=h.ly4b23uays87)

# What is a DPIA and what should it include?

* 1. It is a requirement of the UK General Data Protection Regulations that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.
	2. The UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 make privacy-by-design a key legal requirement, under the term ‘data protection by design and by default’.
	3. The UK GDPR mandates the completion of Data Protection Impact Assessments (DPIA). An effective DPIA will help to ensure that potential data protection and privacy issues and risks are identified at an early stage. This will improve compliance with data protection and privacy laws and standards and uphold the rights and freedoms of living individuals. This formal assessment must be completed from the start of implementing a new system, project, or change.
	4. The Data Protection Impact Assessment (DPIA) is a tool which helps assess data protection and privacy risks to individuals in the collection, use and disclosure of information.
	5. The core principles of conducting a DPIA can be applied to any project, initiative, system or process change which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.
	6. Please note, a DPIA is a living document. Therefore, once a DPIA has been completed and signed off, it is recommended that it is reviewed when any changes are made to the project, initiative, system or process change to ensure that the DPIA is still accurate.
	7. A project which has included a DPIA at the very start of the project, and updated as the project progresses should result in the project being less privacy intrusive and therefore less likely to affect individuals in a negative way.
	8. As part of completing a DPIA, the flow mapping of data must be recorded. Any risks identified by completing the DPIA must be entered onto the relevant organisation’s suitable risk register.
	9. To support you with completing this DPIA template, you may wish to contact your IG lead who may be able to provide copies of completed DPIAs for similar projects. This may be helpful to set out the level of information that is required when completing a DPIA.
	10. Please note, Appendix A provides a list of key definitions which may be helpful to refer to.

#

# Key Details

|  |
| --- |
| Purpose of the Project/Service  |
| Service Name | **Healthtech-1 New Patient Registration Automation** |
| In brief, what is the purpose of the project/service and how is the processing of information necessary to that work?Please include expected outcomes. | **What is the purpose of the project?**The aim of the Healthtech-1’s service is to reduce the time practice staff spend on administration and improve the patient’s experience of engaging with the practice. Healthtech-1’s automated registration product ‘Sanny’ is designed to reduce the ‘time till registration’ for patients, increase the quality and quantity of data collected, and reduce the burden of registrations on the administration team. The need for a DPIA is due to the processing on a large scale of personal and special categories of data for the use of the Healthtech-1 platform.For Healthtech-1 to complete an automated patient registration, the primary data source is from the patient who will manually enter their personal details using their digital device onto the website (typically a computer or mobile).Additional special category data points are collected from the patient for the purpose of increasing quality of care for that patient at the relevant Healthcare Organisation (see appendix C for the full list). A Healthtech-1 developed algorithm then compares the data provided by the patient with the clinical record to verify the identity of the patient.Here Healthtech-1 collects 17 data points from the clinical record (see appendix B) including EMIS number, NHS Number, Date of Birth and Full Name for the purpose of verifying the identity and tracing the patient. The data points are then stored for audit purposes. Knowing what data attributes matched or mismatched at the time of registration is extremely useful should fraud or an incident later be discovered.Furthermore Healthtech-1 will collect anonymised registration, deduction and list size data in order to audit registration volumes and demonstrate impact on practice profitability. This data is collected via a set of EMIS searches, which are viewable under a single folder labelled “Healthtech-1”. This data will be anonymised through aggregation into a report within the Healthtech-1 business intelligence platform, which uses Microsoft Excel.Data is accessed through the Healthcare Organisation’s electronic healthcare record in 2 ways:1. Healthcare Organisation grant specified Healthtech-1 staff smartcard access to each Healthcare Organisation’s clinical system with the “Clerical Access Role” RBAC position (R8010). This is the same role granted to administrators who complete this work in Healthcare Organisation. The purpose of this access is to audit the work of the automated registration software and complete any ad-hoc manual registrations.
2. The Healthtech-1 automation software is also granted access via smartcards assigned to digital assistants, not staff members. Each digital assistant is given the same restricted set of RBAC permissions that abide by the principle of least privilege. This means our automation software has only enough clinical system access to successfully provide the Healthtech-1 automated registration service and no more. This position uses the ‘Admin/Clinical Support Access Role’ RBAC baseline, and each additional activity is declared in Appendix G. These activities have been reviewed by the national PDS team, NHSE National RA and Cyber Operations teams. Using this access, our automation software then registers patients and can be tracked and audited in the same way as all other smartcard users.

**What are the categories of data to flow (e.g. name, age, date of birth, gender)?** Please see appendix C for the full list of data points.Personal Data* NHS Number
* EMIS Number
* Full Name
* Current and previous address
* Gender
* Date of birth
* Contact details
* Emergency contact details
* Previous GP details

Sensitive or Special Category Data* Ethnicity
* Sexuality
* Religion
* Disabilities
* Basic medical data supplied on the medical form (height, weight, BMI, smoking and alcohol status, long term conditions, repeat medication, consent or decline for blood borne virus testing).

**Will you be using identifiable, anonymised or pseudonymised data?**Identifiable data to complete patient registrations, anonymised data for aggregate reporting.**Will the data be used for research, if yes, please provide details?**No. **Is this DPIA for an information system or an App (i.e. an Application for use on an ipad/iphone)? If yes, what is it called?** Sanny, named after the practice administrator who taught us how to do new patient registrations. |

|  |
| --- |
| Timeframe for the Service |
| When is the Service due to begin (planned implementation date)? If it’s time limited, please note the expected end/review date. | The service will start on the date the Healthcare Organisation signs up to the service or on a date they choose to go live. The service will replace business as usual. There is no foreseeable end date.  |

|  |
| --- |
| Nature of the information |
| Will all of the information be truly anonymised information[[1]](#footnote-1)?Anonymised data must meet [the ICO code of practice](https://ico.org.uk/media/1061/anonymisation-code.pdf). | Yes | ☐ | No – some of the information will relate to an identified or an identifiable person (either directly or indirectly) | ☒ |
| Will the information be new information as opposed to using existing information in different ways? | New information |

|  |
| --- |
| **Key Contacts** |
| Key stakeholder names, roles & contact details (can include project management team, developers, information asset owner, data controllers, data processors, system suppliers): | The Healthtech-1 team:*Raj Kohli (Co-founder of Healthtech-1)* *raj@healthtech1.uk**Dr Lydia van Hamel-Parsons(Founding Clinician at Healthtech-1)* *Lydia@healthtech1.uk**Umar Sabat (Independent Data Protection Officer for Healthtech-1)* |

| **Screening Questions** | **YES or NO** |
| --- | --- |
| Will the project involve the collection of information about individuals?  | Yes |
| Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, or have a high impact on the business, whether within a single function or across the whole business? | Yes |
| Will the project compel individuals to provide information about themselves? | Yes |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?  | Yes |
| Are you using personal data/special category data about individuals for a new purpose or in a new way that is different from any existing use?  | No |
| Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make an automated decision about care. | No  |
| Will the project result in you making decisions about individuals in ways which may have a significant impact on them? i.e. does the project change the delivery of direct care.N.B. If the project is using anonymised data only, the response to this question is “No”. | Yes (Decision not considered Privacy Intrusive. Normal patients with a SPINE match are registered automatically. Complex patients i.e. without a match are passed onto practice staff for manual registration.) |
| Will the project require you to contact individuals in ways which they may find intrusive? | No |
| Does the project involve multiple organisations, whether they are public sector agencies accessing personal data/special category data i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners? | Yes |
| Does the project involve new or significantly changed handling of a considerable amount of personal data/special category data about each individual?  | Yes (all new patients registered) |
| Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources? | Yes  |
| Will personal data be processed (e.g. held in a data centre) outside the UK? If yes, please specify the country. | Yes, minimal data processed in EU and US (please see relevant answers below) |
| Does the project relate to data processing which is in any way exempt from legislative privacy protections? E.g. section 251 of the NHS Act 2006. [NHS Digital Link](https://digital.nhs.uk/services/data-access-request-service-dars/how-the-national-data-opt-out-affects-data-released-by-nhs-digital/national-data-opt-out-guidance-for-researchers/appendix-1-section-251-of-the-national-health-service-act-2006%29) | No |

If any of the screening questions have been answered “YES”, then please continue with the full Data Protection Impact Assessment Questionnaire (below). If all questions are “NO”, please return the document to the Information Governance Team and **do not** complete the full Data Protection Impact Assessment.

Please email the completed screening to your information governance lead.

# Controllers[[2]](#footnote-2) and Processors[[3]](#footnote-3)

|  |  |
| --- | --- |
| **Are multiple organisations involved in processing the data?** *If yes, list below and clearly identify where there is a lead Commissioner or Controller.* | Yes/No |
|  |
| Name of Organisation | Controller or Processor? | ODS Code  | Completed and compliant with the DSP Toolkit[[4]](#footnote-4)  |
| Yes/No |
| Health organisations (Healthcare Organisation) | Controller | Varies | Yes |
| Healthtech-1 Ltd. | Processor | A2Q0B | Yes |
| Twilio | Sub-Processor | n/a | No |
| Postmark | Sub-Processor | n/a | No |
| Customer.io | Sub-Processor | n/a | No |
| Microsoft UK | Sub-Processor | 8JH14 | Yes |
| We’ve gone for market leading sub-processors that have strong security controls, with each, we have a Data Protection Addendum to bring them up to GDPR equivalency. [More information about our sub-processors linked here](https://learn-more.healthtech1.uk/sub-processor-softwares). We have also completed a Transfer Risk Assessment (‘TRA’) for sub-processors accordingly. The TRA document assesses and records the risk of transferring data outside of the jurisdiction of the UK. The document can be viewed [here](https://docs.google.com/document/d/1EGGE6P7Qh6t915MoiAROhs9Rd-z2Ms6e/edit?usp=sharing&ouid=116562741349995521371&rtpof=true&sd=true).  |
| **Are there any other organisations involved in this project that are not processing personal data?** **If yes, please name them.**  |
| None |
| **If there is an ICT system provider engaged in this project, please clarify what accreditations they have in place** **(E.g., cyber essentials plus, ISO standards) and whether the Digital Technology Assessment Criteria (DTAC) form has been completed.**  |
| Healthtech-1 use devices provided by North East London ICS to access the secure Health & Social Care Network (HSCN) under a partnership agreement with Stratford Village Surgery. Stratford Village Surgery (F84009) are a [DSPT compliant](https://www.dsptoolkit.nhs.uk/OrganisationSearch/F84009) GP practice with tight [security controls](https://www.notion.so/healthtech1/Partners-bfcc09b54288499d86042204b19752a1) accredited by Cyber Security Essentials. Healthtech-1 has completed their DSPT, certification can be viewed [here](https://www.dsptoolkit.nhs.uk/OrganisationSearch/A2Q0B). Cyber Security Essentials has been approved 01-03-2023. DTAC is planned to be completed by mid-2023. ISO27001 will likely be completed end of 2023/early 2024.**Security measures at sub-processors**Our sub-processors are industry leaders in their service and ensure that they, as well as their sub-processors adhere to high standards. 1. [MS Azure adheres to ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS.](https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance)
2. [Twilio adheres to ISO/IEC 27001, ISO/IEC 27017 & 27018, SOC 2 Type 2, PCI DSS Level 1 and PCI DSS Level 4.](https://www.twilio.com/legal/security-overview)
3. [Customer.IO adheres to CCPA, SOC 2 Type 2, HIPAA and GDPR.](https://customer.io/security/)
4. [Postmark adheres to ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2, and SOC 3, PCI DSS Level 1, and more.](https://postmarkapp.com/eu-privacy#security-and-privacy)

In short, Healthtech-1 has picked suppliers with security controls suitable for healthcare scenarios. We have also completed a Transfer Risk Assessment (‘TRA’) for sub-processors accordingly. The TRA document assesses and records the risk of transferring data outside of the jurisdiction of the UK. The document can be viewed [here](https://docs.google.com/document/d/1EGGE6P7Qh6t915MoiAROhs9Rd-z2Ms6e/edit?usp=sharing&ouid=116562741349995521371&rtpof=true&sd=true).  |
| **Has a data flow mapping exercise been undertaken?***If yes, please provide a copy, if no, please ensure this is completed – speak to your IG Team for guidance* |  |
| Yes – please see below and [Dataflow Diagram Explained - 6th Feb (loom.com)](https://www.loom.com/share/fab4b474ac674c62bda149234cb5085c)  |

# 4. Personal data[[5]](#footnote-5)

|  |
| --- |
| **Use of personal information** |
| If you are intending to use personal data, why would it not be possible to do without personal data? | Personal data is necessary to identify the patient and trace that patient on PDS (the patient demographic service) to register that patient at the Healthcare Organisation. Without this data, the software could not complete a new patient registration (as per the purpose contracted between the Healthcare Organisation and Healthtech-1).Healthtech-1 only collects information from the patient that is either necessary for the purpose of new patient registration, or data from questions that have been designed in collaboration with Healthcare Organisation and agreed with individual Healthcare Organisation in order to serve additional purposes within the Healthcare Organisation e.g. asking about social worker for purposes of child safeguarding or whether the patient would like a blood borne virus screen. This additional, special category data is collected to enrich the Healthcare Organisation’s understanding of the patient’s healthcare needs and circumstances and give them the opportunity to offer more personalised care.The registration form also uses the principles of data minimisation by only requesting and showing relevant data on each load. |
| Is the minimum amount of personal data that is necessary used? | Yes | ☒ | No | ☐ |
| Would it be possible for the Controller/s to use pseudonymised data for any element of the processing? | Yes | ☐ | No | ☒ |
| If Yes, please specify the element(s) and describe the pseudonymisation technique(s) that you are proposing to use and how you will prevent any re-identification of individuals.  | N/A |

|  |
| --- |
| **Description of data: National and local data flows containing personal and identifiable personal information.** What are the required personal data items? |

|  |  |  |  |
| --- | --- | --- | --- |
| **Personal Data**  | **Please tick all that apply** | **Special Category Data** | **Please tick all that apply** |
| Name  | ☒ | Racial or ethnic origin  | ☒ |
| Gender  | ☒ |
| Address (home or business)  | ☒ | Political opinions  | ☐ |
| Postcode  | ☒ | Religious or philosophical beliefs  | ☒ |
| NHS No  | ☒ | Trade union membership  | ☐ |
| Email address  | ☒ | Physical or mental health  | ☒ |
| Sexual orientation  | ☒ |
| Date of birth  | ☒ | Sexual life  | ☐ |
| Payroll number  | ☐ | Criminal offences  | ☐ |
| IP address | ☐ |
| Driving Licence or ID card [shows date of birth and first part of surname]  | ☒ | Biometrics; DNA profile, fingerprints  | ☐ |
| Bank, financial or credit card details  | ☐ | Health, adoption, employment, school, Social Services, housing records | ☒ |
| Mother’s maiden name | ☐ | Child protection  | ☒ |
| National insurance number | ☐ | Genetics | ☐ |
| Tax, benefit or pensions record | ☐ | Safeguarding adults | ☐ |
| Please supply a dummy sample, e.g. blank forms or an itemised list of the data items. | See appendix C for a full list of data points collected. |
| Additional data types (if relevant) | Identification Documents: Patients have the option to upload a photo of ID documents which can also help the GP teams in terms of giving the patient online access to records.Child Protection: in the Healthtech-1 form for 0-15 year olds, it asks about whether the child has a social worker or is fostered. This is to allow Healthtech-1 to safely automate the registrations for children but alert the practice if the child has a social worker for instance. |

|  |
| --- |
| **Lawfulness of the processing** |
| The processing of information must be lawful, and therefore requires a lawful basis. You must choose one or more lawful bases from Article 6 below for processing personal information and one or more from Article 9 below if you are processing special category data (i.e. race, ethnicity, religion, health, sexual orientation, genetic and biometric data, political opinion). Please note: * Choosing ‘consent’ as the lawful basis will overrule all other lawful bases, so only use ‘consent’ where no other lawful basis applies.
* If the purpose of processing is not for direct care, i.e. where personal information is required for secondary uses such as data analysis, reporting etc. Be aware that where a patient has opted-out of their information being used for secondary purposes (i.e. as per the National Data Opt-Out), you will not be able to use their data.

For additional help in deciding the legal basis you can use this interactive tool from the ICO:<https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/>Your IG Team is available to help you identify the legal route for processing data. |
| **Article 6**  | **Article 9** |
| **1(e) Public task** Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*This lawful basis is usually selected for projects to support direct care which process PERSONAL information.*  | ☒ | **2(h) Medical treatment** Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care treatment or management of health or social care systems or a contract with a health professional. *This lawful basis is usually selected for projects to support direct care which process special categories of PERSONAL information.* | ☒ |

|  |  |
| --- | --- |
| If you have chosen consent as your legal basis, describe how you will record consent and its removal if the patient changes their mind?Note: Consent has to be verifiable and cannot be inferred from silence, pre-ticked boxes or inactivity. | Consent is not the identified lawful basis for processing |

|  |
| --- |
| **Describe the information flows** The collection, use and deletion of personal data must be documented.  |
| Does any data flow in identifiable form? If so, from which organisation, and to which organisation/s?Please include a data flow map and confirm the flow has been added to your organisation’s Information Asset and Data flow register. | Please refer to the data flow diagram on Page 12. The user flow:1. Patients access the registration form (henceforth, “the form”) via the practice website. No patient data (for the process of registration) is processed on the website. The website links to the form (test form available [here](https://register-with-gp.ht1.uk/?gpCode=HT1&gpName=Healthtech%201%20General%20Practice)).

On the address portion of the form, the patient can enter in their postcode, and a list of Royal Mail approved addresses is returned. This is using a service called IdealPostcodes (data flow diagram, box 1), and the passing of data is represented by the orange arrow.1. When a patient completes the form, this form data is sent to the Healthtech-1 backend API (box 7). This is a software service that processes data and acts on it when the registration is complete:
	1. It uses the patient's name and email address (if given) to send them a [confirmation email](https://healthtech1.notion.site/Patient-Facing-Messaging-22e78ee83f8a4ac29df2dec1e70c128b) using an EU-based service called Customer.io (box 3.1).
	2. It uses the patient's name and phone number (if given) to send them a [confirmation SMS](https://healthtech1.notion.site/Patient-Facing-Messaging-22e78ee83f8a4ac29df2dec1e70c128b) using a service called Twilio (also represented by box 3.2). This US service is [UK GDPR Compliant](https://www.twilio.com/legal/data-protection-addendum), data processed is encrypted using TLS v1.2 as a minimum.
	3. It sends an email to the designated practice inbox that notifies the practice that a patient has registered and that their full details are available within the Practice Hub (box 11) . The patient's last name and year of birth are provided so the practice can identify which patient the email refers to, and inside the email is a link to that specific registration on the Healthtech-1 Practice Hub. Whilst Postmark and Twilio are both US-based companies and Customer.io is based in the EU, Healthtech-1 have signed data processing addendums with each of these sub-processors, to ensure UK GDPR compliance. Data processed is encrypted in transit for safe passage (HTTPS, TLS, SOC2). See appendix D for a full list of data points processed outside of the UK by these three sub-processors.
	4. The Practice Hub (box 11) is a secure, password protected web-portal where practice staff can access a **full copy** of the patient’s registration.
	5. The backend API also stores the **patient registration form** in a UK database, which is held for audit purposes until the practice ceases to use Healthtech-1 or for 6 years after form submission (as per the Healthtech-1 Data Processing Agreement), whichever occurs soonest (box 8).
		1. Data from the database is aggregated, anonymised and then analysed for business intelligence. Healthtech-1 uses this data to produce monthly anonymised registration reports (box 9).
2. All registration data passed from the backend API (box 7) is processed by Healthtech-1 automation software, built using a Robotic Process Automation (RPA) tool. This RPA tool is provided by Microsoft and runs on the HSCN to input patient data into the clinical system (box 12). Robotic Process Automation is a trusted technology which the [NHS England is introducing to primary care](https://www.nhsx.nhs.uk/key-tools-and-info/guidance-for-designing-delivering-and-sustaining-rpa-within-the-nhs/introduction/).
	1. Healthcare Organisation grant specified Healthtech-1 staff smartcard access to each Healthcare Organisation’s clinical system with the “Clerical Access Role” RBAC position (R8010). This is the same role granted to administrators who complete this work in Healthcare Organisation. The purpose of this access is to audit the work of our automated registration software and complete any ad-hoc manual registrations.
	2. The Healthtech-1 automation software is also granted access via smartcards assigned to digital assistants, not staff members. Each digital assistant is given the same restricted set of RBAC permissions that abide by the principle of least privilege. This means our automation software has only enough clinical system access to successfully provide the Healthtech-1 automated registration service and no more. This position uses the ‘Admin/Clinical Support Access Role’ RBAC baseline and each additional activity is declared in Appendix G. These activities have been reviewed by the national PDS team, NHSE National RA and Cyber Operations teams. Using this access, Healthtech-1 automation software then registers patients and can be tracked and audited in the same way as all other smartcard users.
 |
| What media will you use for the data flow?(e.g. email, post, courier, encrypted hard drive, secure electronic means [e.g. SFTP], other – please specify all that will be used) | Data is transferred via secure transfer protocols such as HTTPS, TLS and SSL to ensure that data in transit is safe and encrypted. Minimal personal data is stored by sub-processors customer.io, Postmark and Twilio in order to send via texts and emails to patients and registration emails to practices (see appendix D). Anonymised, aggregate reports are sent via email to Healthcare Organisations. |

| **Answer all the questions below for the processing of Personal Confidential Data** |
| --- |
| Please identify the conditions under the Data Protection Act 2018 (see Appendix 1 for legal basis under data protection legislation).If you have a Section 251 approval under the NHS Act 2006– please include the approval reference number. If you are relying on consent as your lawful basis, please include a copy of your consent form and identify when and how will this be obtained and recorded? [[6]](#footnote-6)Where there isn’t Section 251 approval, please can you explain how the duty of confidentiality will be met. | The lawful basis of processing lies within Article 6 of the UK GDPR:6(1) ‘Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.And article 9 of the UK GDPR:9(2)(h) ‘…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…’Healthtech-1 has successfully completed the NHS Data Security and Protection Toolkit (DSPT) assurance under NHS ODS code A2Q0B. |
| Where will the data be stored (by the controller(s) and processor(s)? | All Healthtech-1 tools; Form, API, Database, Operations Panel, Practice Hub and Performance Reports and all patient data are stored on MS Azure cloud services located within the UK (South).Limited patient data (see appendix D) is stored in the US using top-grade encryption and security standards (Twilio and Postmark) and EU – Belgium (Customer.io). Twilio keeps logs of sent messages for 30 days, and Postmark keeps logs of practice notification emails for 45 days. Customer.io keeps logs of data until deleted - data is manually deleted on a 30-60 day basis. Healthtech-1 have ensured contractual service agreements and data processing addendums to ensure the sub-processors meet and exceed the standards set by UK GDPR and The DPA 2018. Healthtech-1 has also completed a Transfer Risk Assessment (‘TRA’) for sub-processors accordingly. The TRA document assesses and records the risk of transferring data outside of the jurisdiction of the UK. The document can be viewed [here](https://docs.google.com/document/d/1EGGE6P7Qh6t915MoiAROhs9Rd-z2Ms6e/edit?usp=sharing&ouid=116562741349995521371&rtpof=true&sd=true). Please see Healthtech-1’s public information page on their sub-processors, with access to relevant data processing addendums and whether that sub-processor stores personal or special category data.A list of sub-processor teams or individuals under UK GDPR that have access to Healthtech-1 data is limited and can be found on the [sub-processor information page.](https://learn-more.healthtech1.uk/sub-processor-softwares) |
| How will the data be stored (by the controller(s) and processors(s)? | [Healthtech-1 patient data is stored in MS Azure. MS Azure stores our patient database encrypted at rest using AES-256, with keys managed by Microsoft.](https://learn.microsoft.com/en-us/azure/cosmos-db/database-encryption-at-rest) [Postmark stores data in a Type 2 SSAE 16 SOC 1 accredited facility, where cold data at rest is encrypted with 2048-bit RSA.](https://postmarkapp.com/support/article/917-is-postmark-secure-and-redundant) [Twilio data is encrypted using industry standard encryption algorithms, using strong encryption (volume level, AES-256)](https://support.twilio.com/hc/en-us/articles/360051805394-Measures-Twilio-Takes-to-Safeguard-the-Privacy-of-Customer-Personal-Data)[Customer.io stores data encrypted at rest.](https://customer.io/security/) |
| What confidentiality and security measures will be used to store the data? | Data may be shared with sub-processors such as cloud and digital communication services used for Healthtech-1 storage, communications, security, engineering, and similar purposes. Healthtech-1 sub-processors operate based on Article 28 GDPR-compliant agreements. The majority of data is stored in the UK. The exception to this is that minimal data (see appendix E) is stored by Twilio, customer.io and PostMark to complete text and email messaging to the patient. Special category data is stored solely in the UK and is encrypted when stored using AES-256.**Security measures at Healthtech-1**We apply the NHS Data Security and Protection Toolkit and the Cyber Security Essentials accreditation for protecting and using data appropriately within our organisation. This means employees are trained; organisationally we use firewalls, user access controls, software updates, antivirus to protect our devices and thus access to sensitive data from malicious actors. Each Healthtech-1 employee signs a generic, employment contract with standard confidentiality provisions. They additionally sign a GDPR and Patient Confidentiality agreement. Every team member receives full Primary Care training on confidentiality as provided by Agilio (Teamnet).All Healthtech-1 staff with access to patient data are staff of Stratford Village Surgery an NHS GP practice, and go through the same training and checks .e.g. DBS and Reference checks. With the software that we develop and provide, we follow software engineering best practice and implement security by design to ensure our software service is protected from malicious actors. Finally storage is handled by Microsoft MS Azure, a global leader in IT security and our data is stored within the UK only, encrypted at rest using the highest encryption methods.**Security measures at sub-processors**Our sub-processors are industry leaders in their service and ensure that they, as well as their sub-processors adhere to high standards. [MS Azure adheres to ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS.](https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance)[Twilio adheres to ISO/IEC 27001, ISO/IEC 27017 & 27018, SOC 2 Type 2, PCI DSS Level 1 and PCI DSS Level 4.](https://www.twilio.com/legal/security-overview) [Customer.IO adheres to CCPA, SOC 2 Type 2, HIPAA and GDPR.](https://customer.io/security/)[Postmark adheres to ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2, and SOC 3, PCI DSS Level 1, and more.](https://postmarkapp.com/eu-privacy#security-and-privacy)Healthtech-1 has also completed a Transfer Risk Assessment (‘TRA’) for sub-processors accordingly. The TRA document assesses and records the risk of transferring data outside of the jurisdiction of the UK. The document can be viewed [here](https://docs.google.com/document/d/1EGGE6P7Qh6t915MoiAROhs9Rd-z2Ms6e/edit?usp=sharing&ouid=116562741349995521371&rtpof=true&sd=true). In short, when we pick software to work or integrate with, we pick providers that have security controls suitable for healthcare scenarios.  |
| Who will be able to access personal identifiable data? Please specify the teams (and job titles if possible).  | Healthtech-1 ensures that team personnel accessing the data on Healthtech-1’s behalf are subject to a duty of confidentiality. Access to Personal Data is strictly limited to those employees who strictly require this to perform the Services in the context of that employee's duties to Healthtech-1. Healthtech-1 ensures that their employees:1. are aware of and comply with Healthtech-1’s duties under the company’s Data Processing Agreement with Healthcare Organisation;
2. are informed of the confidential nature of the Personal Data and do not publish, disclose, or divulge any of the Personal Data to any third party unless directed in writing to do so by the Healthcare Organisation or as otherwise permitted by the Data Processing Agreement;
3. are bound by a confidentiality agreement in addition to their employment contract;
4. are subject to user authentication and log on processes when accessing the Personal Data;
5. have undertaken appropriate training in relation to Data Protection Legislation and in the use, care, protection and handling of the Personal Data; and
6. have undertaken appropriate training to process Personal data on behalf of the Healthcare Organisation.

A table of the current members of the Healthtech-1 team:

|  |  |
| --- | --- |
| Name | Job Title |
| Raj Kohli | Head of Growth (Co-Founder) |
| Peter Huang | Head of Product (Co-Founder) |
| Neil Chandarana | Founding Engineer |
| Dr Lydia van Hamel-Parsons | Founding Clinician & NHS GP |
| Rupert Moreton | Founding Operator |
| Dr Dominic Main | Clinical Engineer & NHS GP  |
| Jack Newberry | Software Engineer |
| Eimi Okuno | Software Engineer |
| Matthew Payne | Catalyst |

Healthtech-1 staff may need to access patient data for the following reasons:**Operations:*** During onboarding some practice specific configuration is required, for associating smartcards.
* Investigating a practice stated question about data collected and specific patient related questions.
* Anonymisation and aggregation of practice data in preparing practice reports

**Engineering:*** Configuring the setup of automations for practice specific requirements.
* Debugging
* Investigating incidents

**Other roles:*** Access to manage day-to-day queries
* Investigations of incidents (eg. clinical and data protection)

A table of sub-processor teams who have access to personal or special category data can be found in the [sub-processor information page.](https://learn-more.healthtech1.uk/sub-processor-softwares) |
| How will you consult with the relevant stakeholders? For example, where health data is being processed, has there been a clinical review to consider clinical or ethical impacts/risks of the project? | Dr Lydia van Hamel Parsons and the co-founders of Healthtech-1 spent 6 months completing a vigorous clinical safety review for their automated registration product.As part of the review they consulted a variety of GP practices to understand the clinical and ethical impacts. Their DCB0129 (NHS Digital clinical safety standards for software development) was met on the 27th January 2023. Healthtech-1 are satisfied that the automated registration process represents best in-class clinical safety.  |
| How will you ensure the accuracy and quality of the personal data (including rectification or erasure where necessary)? | The Healthtech-1 patient registration form uses verified Royal Mail Addresses, NHS number, email and phone number validation to improve data entry accuracy including validation on data entry such as height and weight. It also prompts patients to check their answers before submitting their forms through a summary review page. Practices may contact Healthtech-1 at hello@healthtech1.uk to request rectification or removal of patient data. The full policy on this can be read [here](https://learn-more.healthtech1.uk/data-quality-policy).Healthtech-1 keeps patients' data for as long as the Healthcare Organisation continues to use Healthtech-1, for the purpose of providing an auditable service, or for 6 years (as per the Healthtech-1 Data Processing Agreement), whichever occurs soonest.If the Healthcare provider decides to cease services, Healthtech-1 will delete all personal and sensitive patient data, after anonymising and aggregating the data into summary statistics. This aggregation is performed through Healthtech-1’s business intelligence platform. Patient identifiable data is processed by this UK-based service, but the aggregation of this data for report generation anonymises the data. When the report is exported the data is therefore anonymised. E.g. The report may include statistics on patient languages from all forms processed for that practice.Patients may request removal of their data through the Healthcare Organisation who can contact Healthtech-1 at hello@healthtech1.uk to request removal of their data. |
| Will the data be linked with any other data collections? If yes, please explain what data will be linked and what the other data collections are. | In order to complete a new patient registration, the software interacts with the Royal Mail address database, clinical system and PDS (patient demographic service) through the clinical system.. |
| How will this linkage be achieved? | Healthtech-1 automation software connects with the Royal Mail address database (via Ideal Postcodes), clinical system and PDS through the clinical system via the Healthtech-1 API and through the automation software interacting with the clinical system interface via Robotic Process Automation. |
| Is there a legal basis for these linkages? i.e. is the Controller/s responsible for the data expected to cooperate/link data to carry out their legal obligations. | The lawful basis of these linkages lies within Article 6 of the UK GDPR:6(1)(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.The lawful basis of processing special category data lies within Article 9 of the UK GDPR:9(2)(h) ‘…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…’Healthtech-1 has successfully completed the NHS Data Security and Protection Toolkit (DSPT) assurance under [NHS ODS code A2Q0B.](https://www.dsptoolkit.nhs.uk/OrganisationSearch/A2Q0B)These linkages are necessary for the automation software to perform the new patient registration and therefore for Healthtech-1 to meet with their contractual obligation to perform this service for the Healthcare Organisation. |
| Do you have a process in place and/or system functionality to respond to the right to data portability requests? | Healthtech-1 has ensured that should a patient wish to request a copy of their data they can do so through the Healthcare Organisation who would notify Healthtech-1. The request would be verified, and then the relevant data would be extracted to csv, protected by a password and then encrypted and sent electronically to the Healthcare Organisation to provide to the data subject. |
| What security measures will be used when the data is in transit? | MS Azure - TLS 1.2Twilio - TLS 1.2Customer.io - 128-bit SSLPostmark - 256-bit SSLData processed is encrypted in transit for safe passage . Please see more information on the [Healthtech-1 sub-processor page](https://learn-more.healthtech1.uk/sub-processor-softwares). |
| How long will the data be retained in identifiable form? How will it be de-identified or destroyed? Who will be responsible for ensuring the data is de-identified or destroyed?  | Healthtech-1 retains data in identifiable form for the length of the contract with the Healthcare Organisation or for 6 years, whichever occurs soonest. Healthtech-1 must delete or return all Personal Data to the Healthcare Organisation, at the choice of the Healthcare Organisation, as requested at the point of termination of their Data Processing Agreement and Healthtech-1 will provide confirmation that all copies of the Personal Data have been deleted within 90 days after termination of the relevant Data Processing Agreement. Prior to deletion, Healthtech-1 will anonymise and aggregate the data into summary statistics. This anonymised data is used by Healthtech-1 for evidence generation, reporting service metrics, business intelligence and analysing trends or patterns in the data (such as patient language needs or reasons for moving Healthcare Organisation). Healthtech-1 anonymises this data at the point of aggregation by deleting personally identifiable information. |
| What governance and assurance measures are in place to ensure the confidentiality, security and appropriate use of the data? E.g. policies and procedures, system security policy, information asset register, accountability roles identified  | Practices and Healthtech-1 agree to a Data Processing Agreement (provided) which specifies how and why Healthtech-1 will be processing patient data. This DPIA template will be provided to surgeries once approved.Healthtech-1 has successfully completed the NHS Data Security and Protection Toolkit (DSPT) assurance under [NHS ODS code A2Q0B.](https://www.dsptoolkit.nhs.uk/OrganisationSearch/A2Q0B)The internal log of Healthtech-1 DSPT assurances can be made available on request, including data security and protection policies and procedures, information asset register and assignment of responsibilities.Please see the answer to *“Who will be able to access personal identifiable data? Please specify the teams (and job titles if possible)”* to learn more about assurance measures for all Healthtech-1 personnel. **Sub-processor assurances**Sub processors chosen are leaders in their industry and thus have aligned their security and data protection to national compliance standards. Healthtech-1 has also completed a Transfer Risk Assessment (‘TRA’) for sub-processors accordingly. The TRA document assesses and records the risk of transferring data outside of the jurisdiction of the UK. The document can be viewed [here](https://docs.google.com/document/d/1EGGE6P7Qh6t915MoiAROhs9Rd-z2Ms6e/edit?usp=sharing&ouid=116562741349995521371&rtpof=true&sd=true). [MS Azure adheres to ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS.](https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance)[Twilio adheres to ISO/IEC 27001, ISO/IEC 27017 & 27018, SOC 2 Type 2, PCI DSS Level 1 and PCI DSS Level 4.](https://www.twilio.com/legal/security-overview) [Customer.IO adheres to CCPA, SOC 2 Type 2, HIPAA and GDPR.](https://customer.io/security/)[Postmark adheres to ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2, and SOC 3, PCI DSS Level 1, and more.](https://postmarkapp.com/eu-privacy#security-and-privacy)Adherence to the NHS DSP Toolkit can be found in the first table of Section 5. |
| What are the contractual arrangements for this project? E.g. NHS standard contract, data processing agreement, data sharing agreement  | Healthtech-1 contracts with each Healthcare Organisation via a Service Agreement which includes an agreement to data processing, held within the Data Processing Agreement. |
| Where there are sub-processors engaged for the project, do you have assurance that the processor(s) has a contract with their sub-processor(s)?  | Healthtech-1 makes this information available on a public information page that can be reviewed, with copies of sub-processor contracts and Data Addendums. |
| Do you need to consider consulting information technology experts as part of this change process/project? i.e. IT Infrastructure or software deployment, ICT resources/knowledge and skills. | No, the software is simple to integrate and use. |
| Please embed a copy of the System Level Security Policy (SLSP) for the project/service.This policy needs to identify the technical controls that enable you to demonstrate that you have ensured privacy by design has been addressed by ensuring you have information on the controls required to protect the data.  | Healthtech-1 has successfully completed the NHS Data Security and Protection Toolkit (DSPT) assurance under NHS ODS code A2Q0B. The System Level Security Policy (SLSP) can be [found here.](https://docs.google.com/document/d/1m36YHOj7vNR3LCvgYbTUhClhppK1VyT49tPxe4nFBuw/edit?usp=sharing) |
| If holding personal i.e. identifiable data, are procedures in place for subject access requests? | Yes. Healthtech-1 has ensured that should a patient wish to request a copy of, rectification or removal of their data they can do so through the Healthcare Organisation who would notify Healthtech-1 at hello@healthtech1.uk. The request would be verified, and then the relevant data would be extracted to csv, protected by a password and then encrypted and sent electronically to the Healthcare Organisation to provide to the data subject.If relevant to the request (objection, withdrawal of consent) then in agreement with the Healthcare Organisation, the data would be deleted. |
| Are there any plans to allow the information to be used elsewhere either in the wider NHS or by a third party? If so, please explain.  | Data will be shared with practice staff that are responsible for managing and processing patients’ registrations at each Healthcare Organisation. Anonymised and aggregated data may be shared with PCN, ICB, ICSs or other NHS stakeholders. An example, we might share anonymised and aggregated ‘translation needs’ data with an ICS, so they can design interventions to support practices. As a matter of principle, we would avoid sharing data that might bring a practice into disrepute or for performance management. Software usage data is collected by Healthtech-1 (anonymised data) and used to improve their products and services. This data focuses on service metrics, for example how many registrations have been automated, how many have been manually completed by the practice, time taken to complete an automated registration from patient form submission through to registration completion in the clinical system.Data may be shared with sub-processors such as cloud and digital communication services used for Healthtech-1 storage, communications, security, engineering, and similar purposes. Healthtech-1 sub-processors operate based on Article 28 GDPR-compliant agreements. Storage of special category data by Healthtech-1 is UK-based only. The majority of personal data is stored in the UK, but a minimal amount (see appendix D) is also stored in either the EU - Belgium ([Customer.io](http://customer.io)) or the USA (Postmark and Twilio). Please also see data flow diagram (page 11). Data processing addendums and contracts between Healthtech-1 and these three suppliers that process data out of country are in the sub-processor page. |
| Will the privacy notices in relation to this data be updated and ensure it includes:* ID of controller
* Legal basis for the processing
* Categories of personal data
* Recipients, sources or categories of recipients of the data: any sharing or transfers of the data (including to other countries)
* Any automated decision making
* Retention period for the personal data
* Existence of data subject rights, including access to their data and/or withdrawal of consent and data portability
 | Healthcare Organisations should update their privacy notices to state that they are working with Healthtech-1 to automate patient registrations. The registration form has a privacy policy button which directs patients to the latest information about how their data is handled. The latest version can always be found [here](https://docs.healthtech1.uk/privacy-policy) and it would be advisable for Healthcare Organisations to link to this in their privacy notice too. |
| Where consent or contractual arrangements is the lawful basis for processing and your project involves automated processing, how will you ensure you can separate some data from other datasets if required, to enable data portability?  | Data that has been automatically processed is associated with metadata in the Healthtech-1 database that identifies the individual patient and the individual Healthcare Organisation, therefore separating this data from other datasets is a simple process. |

#

# Access and reporting

|  |
| --- |
| **How many members of staff will have access to the data? Please can you also explain the access controls in place.**  |
| 9 members of staff will have access to the data. There are 4 ways in which data can be accessed:1. Healthtech-1’s automation software is granted access via smartcards assigned to digital assistants, not staff members. Each digital assistant is given a restricted set of RBAC permissions that abide by the principle of least privilege (Appendix G). This means our automation software has only enough clinical system access to successfully provide the Healthtech-1 service and no more. Our automation software then registers patients using these restricted smartcards and can be tracked and audited in the same way as all other smartcard users. These smartcards are plugged into smartcard readers stored in an accredited safe and connected to HSCN-connected desktops protected by security controls accredited by the Cyber Security Essentials framework.
2. Healthcare Organisations grant Healthtech-1 Operations staff smartcard access to each Healthcare Organisation’s clinical system with the “Clerical Access Role” RBAC position (R8010). This is the same role granted to administrators who complete this work in Healthcare Organisation. The purpose of this access is to audit the work of our automated registration software and complete any ad-hoc manual registrations.
3. The Healthtech-1 Engineering staff have internal database access for audit and operational work core to the development and maintenance of the registration product. New access must pass an approval process that involves leadership. All user accounts are audited on a regular basis. Access is secure and requires multi-factor authentication.
4. Healthcare Organisation staff have access to registration form data using accounts to our portal. Accounts are set up for specified individuals at Healthcare Organisation. Accounts are approved, created and managed by the Healthtech-1 staff.
5. Data as previously mentioned is stored in a secure, UK based, encrypted database. To complete important operational work and view this data, access is provided by a software called Retool. Retool account allocation passes through an approval process that involves leadership, and access is secure and multi-factor. User account access is audited on a regular basis. We run Retool within a UK based server which means data always remains within the UK.
 |
| **What access controls will you have in place to ensure there is only authorised access to the data?** **Please include your procedure for enabling access, removing access, monitoring access and identifying any inappropriate access.** |
| Data accessible through the practice’s electronic healthcare record (EMIS or SystmOne):Healthcare Organisation grant Healthtech-1 Operations staff smartcard access to each Healthcare Organisation’s clinical system with the “Clerical Access Role” RBAC position (R8010). The purpose of this access is to audit the work of our automated registration software and complete any ad-hoc manual registrations. Some examples of when manual interventions might occur include completing a registration manually under instruction from the Healthcare Organisation, to update clinical system settings (e.g. Usual GP), or if the automation software fails and needs intervention. Smartcard access can be monitored and RBAC positions can be revoked by the Healthcare Organisation if the Healthcare Organisation has an allocated Registration Authority Sponsor (RA Sponsor) or by the Registration Authority local to the Healthcare Organisation (ICB RA).Healthtech-1’s automation software is granted access via smartcards assigned to digital assistants, not staff members. Each digital assistant is given a restricted set of RBAC permissions that abide by the principle of least privilege (Appendix G). This means our automation software has only enough clinical system access to successfully provide the Healthtech-1 service and no more. Smartcard access can be monitored and RBAC positions can be revoked by the Healthcare Organisation if the Healthcare Organisation has an allocated RA Sponsor, or by the ICB RA local to the Healthcare Organisation. Using restricted access, our automation software then fulfils the automated registration service and can be tracked and audited in the same way as all other smartcard users. Healthtech-1 follow published NHS guidance on secure authentication using automation (link below). Specific security controls include:* Healthtech-1 use one smartcard per automation desktop
* Healthtech-1 smartcards are plugged into smartcard readers stored in an accredited safe in a secure location
* connected to HSCN-connected desktops protected by security controls accredited by the Cyber Security Essentials framework
* Healthtech-1 use a standardised naming convention and image format for printing on smartcard
* Multiple smartcards are dedicated to complete registrations at each practice for improved capacity and resilience.

<https://digital.nhs.uk/services/care-identity-service/registration-authority-users/registration-authority-help/secure-authentication-for-robotic-process-automation>Healthtech-1 team members:1. are aware of and comply with Healthtech-1’s duties under the company’s Data Processing Agreement with Healthcare Organisation;
2. are informed of the confidential nature of the Personal Data and do not publish, disclose, or divulge any of the Personal Data to any third party unless directed in writing to do so by the Healthcare Organisation or as otherwise permitted by this Data Processing Agreement;
3. are bound by a confidentiality agreement as per their employment contract;
4. are subject to user authentication and log on processes when accessing the Personal Data;
5. have undertaken appropriate training in relation to Data Protection Legislation and in the use, care, protection and handling of the Personal Data; and have undertaken appropriate training to process personal data on behalf of the Healthcare Organisation.

Data accessible through the Healthtech-1 database:Access to the Healthtech-1 database is restricted to members of the team who require access to complete engineering and operational duties as employees of Healthtech-1 so that the company can complete new patient registrations. The operations panel allows a view into this database and access to patient registration data. Account management for both of these services is managed by Peter Huang, who is responsible for data protection and security at Healthtech-1. Accounts are generated for team members who require access to complete their duties as employees of Healthtech-1. Account access is protected by two factor authentication.Data accessible through the Practice Hub:Healthcare Organisation staff Practice Hub access is log in protected and access is set up for specified individuals at Healthcare Organisations. Healthtech-1 team members do not have Practice Hub log in details for individual practices, therefore patient data cannot be accessed by Healthtech-1 team members through this means. Practice Hub logins are stored in a secure, encrypted database on a Healthtech-1 sub-processor platform, which is UK-based.Organisationally, we apply the Cyber Security Essentials framework for account access controls. All account creation goes through senior management with area ownership. Admin accounts and accounts that can access sensitive data go through a stricter approval process and involve top leadership. In this process, evaluation of risk, allocation of permissions on a model of least privilege is used. If the account is approved, documentation of access is logged, and strong security controls will be applied such as strong passwords and multi-factor authentication. Access control is also regularly audited with a primary focus on accounts with access to sensitive data. We use modern tools which have automated technical controls, which alert the IT admin (Peter Huang) to suspicious account activity, as well as preventing access if such activity continues. Unapproved or suspicious activity will be challenged and investigated by Peter Huang, Healthtech-1’s Security Lead.  |
| **Are there any new or additional reporting requirements from the system/software being used for this project/service?** **If “No” move to section 5 below: Business Continuity planning**  |
| 1. Monthly practice reports:

Data from the database is aggregated, anonymised and then analysed for business intelligence. Healthtech-1 uses this data to produce monthly registration reports. Monthly reports quantify service performance, for example numbers of automated versus manual registration and average time to complete registration. The data remains identifiable in the Healthtech-1 business intelligence platform (UK-based) and this service is used to produce an aggregated report (per practice) that only contains anonymised data. Anonymisation is achieved by partial data removal of Name, DOB, address, gender, NHS number, title. This report is then distributed to each relevant practice. 1. Evidence generation:

Anonymised data is used by Healthtech-1 for evidence generation, reporting service metrics, business intelligence and analysing trends or patterns in the data (such as patient language needs or reasons for moving Healthcare Organisation). Healthtech-1 anonymises this data at the point of aggregation by deleting personally identifiable information leaving it’s business intelligence platform |
| **Will the reports be in sensitive or redacted format (removing anything which is sensitive) format?** |
| Yes where required. |
| **Will the reports be in person-identifiable, pseudonymised or anonymised format?** |
| Anonymised. |
| **What roles will be able to run reports? E.g. service activity reports, reports on individual people.** |
| The primary Healthtech-1 employee who runs service activity reports is the Founding Operator, Rupert Moreton. Dr van Hamel-Parsons (Founding Clinician) may also run reports as part of the evidence generation described above. |
| **What roles will receive the report or where will it be published? Please can you also clarify the names of the organisations.**  |
| Practice reports are sent via email to the lead contacts at individual Healthcare Organisation. Anonymised and aggregated data may be shared with PCN, ICB, ICS or other NHS stakeholders. |
| **If this new/revised reporting function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?** |
| As the reports contain anonymised, aggregate information, this does not apply. |
| **What plans are in place in relation to the internal reporting of a personal data breach?****(NB A personal data breach may need to be reported to the ICO within 72 hours. Therefore, it is recommended that plans are in place to report a data breach to the relevant organisations within 24-48 hours.)** |
| The Healthtech-1 business continuity plan can be read at [this link](https://learn-more.healthtech1.uk/data-security-compliance/business-continuity-plan-data-and-cyber-security). The Healthtech-1 policy in relation to the internal reporting of a personal data breach can be found [here](https://learn-more.healthtech1.uk/data-security-compliance/guidance-on-security-breaches). Healthtech-1 will report to affected parties within 24 hours. Their goal would be to act swiftly and effectively, while upholding best practice, uppermost care and duty of candour.  |
| **What plans are in place in relation to the notification of data subjects should there be a personal data breach?** |
| 1. Discuss with the DPO whether the patient is owed Duty of Candour (most likely yes), and what level of duty of candour and means of communication is appropriate in the situation.
2. Personnel responsible for managing Data and Security Protection at Healthtech-1 would inform the Healthcare Organisation as the Data Controller to facilitate performance of duty of candour and apology to the Data Subject.
3. We would inform the Healthcare Organisation of three things as part of an apology:
* What happened.
* What can be done to deal with any harm caused, including recommendations to mitigate potential adverse effects.
* What will be done to prevent someone else experiencing the same issue.
 |

#

# Business continuity planning

|  |
| --- |
| **How will the personal data be restored in a timely manner in the event of a physical or technical incident?** |
| Healthtech-1 has hourly data backups on Microsoft MS Azure.To restore this data, Healthtech-1 would contact MS Azure support, who would release a copy of the data and support Healthtech-1 to reinstate their database. |
| **How business critical is the system you are using – tick only one:** |
| ☐ Tier 1 – Critical (restoration asap within 24 hrs) X Tier 2 – Significant (restoration within 24-48 hrs) ☐ Tier 3 – Moderate (restoration within 1 week)☐ Tier 4 – Minor (restoration over 1 week) |

#

# Direct marketing[[7]](#footnote-7)

|  |
| --- |
| **Will any personal data be processed for direct marketing purposes?****If Yes, please describe how the proposed direct marketing will take place:*****If you would like further information about what direct marketing is, please refer to the ICO guidance:* *https://ico.org.uk/media/1555/direct-marketing-guidance.pdf*** |
| No |

# Automated processing

|  |
| --- |
| **Will the processing result in a decision being made about the data subject solely because of automated processing[[8]](#footnote-8) (including profiling[[9]](#footnote-9))?** |
| The processing will result in a decision being made about a subject - whether they will be automatically registered or passed over to the practice for manual registration/investigation. An algorithm verifies the identity of a patient and matches them against an existing NHS record. If it cannot match the record against an existing NHS record, then a “decision” is made for the registration to automatically pass over to the practice to be manually registered. Deciding if patient-supplied data matches an existing NHS record is necessary for a Healthcare Organisation to register a patient. For the avoidance of doubt, Healthtech-1 does not make an automated decision as to whether the patient can be registered at the Healthcare Organisation.  |
| **If Yes, is the decision:*** **Necessary for entering into, or performance of, a contract between the data subject and a data controller**
* **Authorised by law**
* **Based on the data subject’s explicit consent?**

**Please describe the steps involved in any automated decision-making including any human intervention in monitoring this.** |
| Patient matching is the process of linking a patient to their clinical record. Before Healthtech-1 updates any medical record to register a patient, that patient-record pair must first successfully pass through the scrutiny of a patient match algorithm. The algorithm compares up to 17 attributes from the patient’s registration form against the NHS database of medical records across 3 tiers of tests. The 3 tiers represent categories of attributes:1. Demographic2. Contact details3. Personal detailsThe end result is either a pass or a fail. If the patient-record pair passes, Healthtech-1 continues with the registration. If it fails, Healthtech-1 passes the registration over to the Healthcare Organisation to complete. |

# Risk Management and action plan

The risk score will determine the level of authorisation needed for any DPIA completed that requires a full DPIA.

Any risk score that is verified by the IG team to be in the upper range of a medium risk score (9 to 12) or in the range of high risk will require referral to the relevant Data Protection Officer for review and comment.

DPIA risks that score as high risk will only have the processing of the data approved by the relevant SIRO and Caldicott Guardian once the risk has been mitigated to reduce the risk to medium as a minimum. Where this is not possible, a high-risk score will also require escalation to and a response from NHSE&I and the Information Commissioner’s Office before any processing can commence.

The escalation process also includes a review to enable the risk to be lowered to within tolerance, if possible. The table below identifies the ranges for the scores and the risk level associated with each range of scores.



|  |  |
| --- | --- |
| **Data Protection Risks** List any identified risks to Data Protection and personal information of which the project is currently aware. Risks should also be included on the project risk register. |  |
| **Risk Description****(to individuals, to the organisation(s) involved or to wider compliance)** |  **Impact** | **Likelihood** | **Risk Score (I x L)** | **Proposed Risk solution (Mitigation)** | **Is the risk reduced,transferred, or accepted? Please specify.** | **Evaluation: is the final****impact on individuals****after implementing each****solution a justified,****compliant and****proportionate response****to the aims of the project?** | **Actions to be taken (please include target date for completion and action owner)** | **Comments from IG lead**  | **Comments from Information Security lead (where applicable)**  |
| Malicious actor registers pretending to be someone else. | 4 | 2 | 8 | Each patient registration undergoes ID checks and would fail patient match (where patient identity is verified and traced on the patient demographic service, PDS). | Reduced | Yes | NA |  |  |
| Healthtech-1 will be able to access practice patient data through smartcard access, increasing the likelihood of a data breach. Each individual Healthcare Organisation grants access to specified Healthtech-1 team members. It is required to enable access for the automation software to complete an automated registration. | 4 | 2 | 8 | Healthtech-1 personnel are provided with limited access through the “Clerical Access Role” RBAC position. The activity of the user of the smartcard is auditable in the same way that internal Healthcare Organisation staff members activity is auditable. Healthcare Organisation have full control over smartcard access. Access can be revoked at the Healthcare Organisation level or by the Registration Authority local to the Healthcare Organisation (ICB level).All Healthtech-1 personnel have completed Information Governance, Data Security and Cybersecurity mandatory training modules. Additionally all staff:1. are aware of and comply with Healthtech-1’s duties under the company’s Data Processing Agreement with Healthcare Organisation;
2. are informed of the confidential nature of the Personal Data and do not publish, disclose, or divulge any of the Personal Data to any third party unless directed in writing to do so by the Healthcare Organisation or as otherwise permitted by this Data Processing Agreement;
3. are bound by a confidentiality agreement as per their employment contract;
4. are subject to user authentication and log on processes when accessing the Personal Data;
5. have undertaken appropriate training in relation to Data Protection Legislation and in the use, care, protection and handling of the Personal Data; and
6. have undertaken appropriate training to process Personal data on behalf of the Healthcare Organisation.
 | Reduced | Yes | NA |  |  |
| Practice staff copy and paste the wrong information across into the clinical system | 4 | 2 | 8 | Within the Practice Hub, a clear visual indicator of what information has been copied appears in the right-hand corner of the screen, additionally the selected patient’s name is clearly displayed in portal at the top of the screen, one click copy function in portal so that e.g. NHS number or date of birth can be copied across to the clinical system to search for the correct patient accurately. | Reduced | Yes | NA |  |  |
| The integrity of the computers used (how at risk are they from trojans or viruses) | 3 | 2 | 6 | The machines used by Healthtech-1 for automation work are networked within HCSN, the physical machines are housed within a GP practice in Newham, these machines are subject to North East London IT security and anti-virus policies and practices.Local security measures include: building security and alarm system; multiple layers of locks (building front door lock, stairwell lock/ key card access, office room lock, device lock).Our operational room is not accessible to the public. Room access is restricted to working personnel only, with access key card and physical 6 digit combination locks on office doors preventing unauthorised access. Our room is also always attended by multiple employees, and when empty the room is always locked. | Reduced |  |  |  |  |
| Patient data accessed by an inappropriate / malevolent user, external hacker or Healthtech-1 employee | 5 | 2 | 10 | Access to the clinical system is restricted to specified Healthtech-1 team Smartcards, Healthtech-1 enforce mandatory training for their employees on data security, cyber security and information governance. DBS checks have been completed on every Healthtech-1 employee, DSPT has been completed and Healthtech-1 are working towards CSE and DTAC sign off. | Reduced | Yes | No |  |  |
| Practice staff abuse the free text communication features (SMS and email) with risk of patient’s contact data being used inappropriately and in a way in which patients may find intrusive. | 4 | 1 | 4 | Portal access (through which SMS and emails can be triggered) is log-in protected and access is set up for specified individuals at Healthcare Organisations. There is an audit trail of the messaging sent and by whom. Additionally, the API is throttled to prevent high-frequency, repetitive triggering of messaging events. | Reduced | Yes | No |  |  |
| Access to personal data by persons other than the data subject | 4 | 2 | 8 | Healthcare Organisation grant Healthtech-1 staff smartcard access to each Healthcare Organisation’s clinical system with the “Clerical Access Role” RBAC position (R8010). This is the same role granted to administrators who complete this work in Healthcare Organisation. The purpose of this access is to audit the work of our automated registration software and complete any ad-hoc manual registrations.Healthtech-1’s automation software is granted access via smartcards assigned to digital assistants, not staff members. Each digital assistant is given a restricted set of RBAC permissions that abide by the principle of least privilege. This means our automation software has only enough clinical system access to successfully provide the Healthtech-1 service and no more. Our automation software then registers patients using these restricted smartcards and can be tracked and audited in the same way as all other smartcard users. These smartcards are plugged into smartcard readers stored in an accredited safe and connected to HSCN-connected desktops protected by security controls accredited by the Cyber Security Essentials framework.The activity of both human users and automation software smartcards are auditable in the same way that internal Healthcare Organisation staff members activity is auditable. Healthcare Organisation and ICB RA teams retain the ability to revoke smartcards. All Healthtech-1 personnel have completed Information Governance, Data Security and Cybersecurity mandatory training modules. Additionally all staff:1. are aware of and comply with Healthtech-1’s duties under the company’s Data Processing Agreement with Healthcare Organisation;
2. are informed of the confidential nature of the Personal Data and do not publish, disclose, or divulge any of the Personal Data to any third party unless directed in writing to do so by the Healthcare Organisation or as otherwise permitted by this Data Processing Agreement;
3. are bound by a confidentiality agreement as per their employment contract;
4. are subject to user authentication and log on processes when accessing the Personal Data;
5. have undertaken appropriate training in relation to Data Protection Legislation and in the use, care, protection and handling of the Personal Data; and
6. have undertaken appropriate training to process Personal data on behalf of the Healthcare Organisation.
 | Reduced | Yes | No |  |  |
| The provider (Healthtech-1) utilises processors that store data outside of the UK. Data is stored in the EU and the US. The risk is that patient could be compromised by sub-processors. | 4 | 2 | 8 | Proposed Risk solution (Mitigation)Healthtech-1, uses sub-processors outside of the UK to provide the best possible service to practices. Each sub-processor is secure:[Twilio adheres to ISO/IEC 27001, ISO/IEC 27017 & 27018, SOC 2 Type 2, PCI DSS Level 1 and PCI DSS Level 4.](https://www.twilio.com/legal/security-overview) [Customer.IO adheres to CCPA, SOC 2 Type 2, HIPAA and GDPR.](https://customer.io/security/)[Postmark adheres to ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2, and SOC 3, PCI DSS Level 1, and more.](https://postmarkapp.com/eu-privacy#security-and-privacy)Healthtech-1 has signed Data Addendums to bind each sub-processor to UK GDPR data treatment standards and has completed a Transfer Risk Assessment accordingly ([here](https://docs.google.com/document/d/1EGGE6P7Qh6t915MoiAROhs9Rd-z2Ms6e/edit?usp=drive_link)).  | Reduced | Yes | Transfer off US sub-processors (Twillio & Postmark) to UK alternatives, after a technical evaluation.July 2024 - Peter Huang (Co-founder & Head of Product)  |  |  |

# Reviewed By

**This DPIA has been last reviewed by the following individuals:**

|  |  |  |
| --- | --- | --- |
| **Name** | **Job Title** | **Date** |
| Rajkumar Kohli | Co-founder at Healthtech-1 | 24/02/2023 |
| Matthew Payne | Catalyst at Healthtech-1 | 05/09/2023 |
| Aaron Cameron | Assistant Practice Manager of Beech Tree Surgery | 11.09.2023 |
|  |  |  |
|  |  |  |

# Appendix A: Definitions and Glossary

**Definitions**

DPIA             Data Protection Impact Assessment

UK GDPR   UK General Data ProtectionRegulations

ICO             Information Commissioner’s Office

DPO            Data Protection Officer

**Glossary**

**Anonymisation**

Anonymisation is the process of rendering data into a form which does not identify individuals, and where identification is not likely to take place. By definition, anonymised data do not relate to a particular individual any more than they relate to anyone else in the underlying population.

**Biometric data**

‘Biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (finger print) data;

**Business sensitive data**

“Business sensitive” relates to information and documentation which is created, that requires confidentiality due to the legal, ethical or commercial content.  Information that, if disclosed, could prejudice, or cause reputational or financial damage to an organisation.

**Consent**

‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

**Cyber Essentials**

A government accredited set of basic technical controls to help organisations protect themselves against common online security threats.  The scheme enables organisations to gain one or two Cyber Essential badges and is suitable for organisations of any size, in any sector <https://www.cyberessentials.ncsc.gov.uk/>

**Data portability**

‘The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability’.

**Genetic data**

‘Genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

**ISO 27001**

ISO 27001 is the international standard that provides specification for best-practice information security management systems (ISMS). It provides a certificated accreditation and is supported by a code of practice for information security management.

**Lawful basis for processing**

The lawful bases for processing are set out in Article 6 of the General Data Protection Regulations.  At least one of the lawful basis for processing must apply whenever you process personal data. (see appendix B for a full list).

**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;

**Pseudonymisation**

Pseudonymisation is 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.

**Special categories of data**

Special categories of data are considered as more sensitive data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

# Appendix B: Data points stored and used to match patients to the clinical record.

1. NHS number
2. First name
3. Last name
4. Gender
5. Same sex at birth yes/no
6. DoB
7. Email
8. Mobile number
9. Home number
10. Previous postcode
11. Current postcode
12. Temporary postcode
13. Previous GP
14. Title
15. Ethnicity
16. Religion
17. Country of birth

#

# Appendix C: Full list of data points collected and stored from the patient registration forms

|  |  |
| --- | --- |
| catchmentPostcode | emergencyContactTitle |
| title | emergencyContactFirstName |
| firstName | emergencyContactLastName |
| middleName | emergencyContactGender |
| lastName | emergencyContactEmail |
| email | emergencyContactContactNumber |
| mobileNumber | emergencyContactRelationship |
| homeNumber | emergencyContactStartedPermissionOfCare |
| cioEmail (customer.io generated email) | emergencyContactLivesWithPatient |
| registrationFor | emergencyContactCanDiscussMedicalRecords |
| registrationReason | emergencyContactIsCarer |
| representativeTitle | emergencyContactIsPatientAlready |
| representativeFirstName | hasHadPreviousNames |
| representativeLastName | previousFirstNames |
| representativeGender | previousLastNames |
| representativeEmail | hasMoved |
| representativeContactNumber | previousAddressLine1 |
| representativeRelationship | previousAddressLine2 |
| nhsNumber | previousAddressLine3 |
| gender | previousCounty |
| isSameSexAtBirth | previousDependantLocality |
| sexualOrientation | previousWard |
| religion | previousPostTown |
| dateOfBirth | previousPostcode |
| ethnicity | isFirstGp |
| comingBackFromLivingAbroad | previousGpCode |
| lastLeaveUk | previousGpName |
| lastReturnUk | keepPharmacy |
| ukBorn | preferredContactMethod |
| birthCountry | contactConsent |
| firstLiveUk | has\_repeatMedications |
| needsInterpreter | repeatMedications |
| interpreterLanguage | longTermConditions |
| isArmedForces | wantsBBVScreening |
| armedForcesRole | specialCircumstances |
| enlistmentDate | hasDisabilities |
| attendsEducationalInstitution | disabilityDescription |
| educationalInstitutionType | weightKg |
| educationalInstitution | heightCm |
| hasSiblingWithSameDateOfBirth | BMI |
| isFostered | hasAllergies |
| hasSocialWorker | allergies |
| socialWorkerName | exerciseFrequency |
| socialWorkerContactNumber | smokingStatus |
| socialWorkerEmail | dailySmokingFrequency |
| roomNumber | wantsSmokingAdvice |
| addressLine1 | alcoholStatus |
| addressLine2 | alcoholOverGuidelineFrequency |
| addressLine3 | alcoholFailedToActNormally |
| postTown | alcoholLostMemory |
| county | alcoholConcernFromOthers |
| dependantLocality | FAST Score |
| ward | offeredHIVTest |
| postcode | wantsHIVTest |
| longitude | wantsChlamydiaTest |
| latitude | ppgConsent |
| livesInCareOrNursingHome | documents |
| summaryCareRecordConsent | ageAtFormSubmission |
| childRegWithoutpersonOfParentalResponsibility | withinPracticeCatchment |
| livesWithperson of parental responsibility | usualGp |
| person of parental responsibilityTitle |  |
| person of parental responsibilityFirstName |  |
| person of parental responsibilityLastName |  |
| person of parental responsibilityGender |  |
| person of parental responsibilityDateOfBirth |  |
| person of parental responsibilityContactNumber |  |
| person of parental responsibilityEmail |  |
| person of parental responsibilityRelationship |  |
| person of parental responsibilityIsPatientAlready |  |
| person of parental responsibilityRoomNumber |  |
| person of parental responsibilityAddressLine1 |  |
| person of parental responsibilityAddressLine2 |  |
| person of parental responsibilityAddressLine3 |  |
| person of parental responsibilityDependantLocality |  |
| person of parental responsibilityWard |  |
| person of parental responsibilityPostTown |  |
| person of parental responsibilityCounty |  |
| person of parental responsibilityPostcode |  |

#

# Appendix D: Full list of data points collected and stored by customer.io (EU), Twilio and Postmark

These data points are used to send personalised messaging (text and email) to patients. Examples include but are not limited to:

1. sending a confirmation of form receipt email
2. sending welcome emails with their new GP’s details
3. asking for more documentation because we are their first GP
4. suggesting that patients fill in the medical form
5. telling parents about their child’s registration
6. fulfil patient requests. E.g. with wantsSmokingAdvice, we send them a link to a local smoking cessation advice resource

**Customer.io:**

**Personal Data**

* firstName
* lastName
* mobileNumber
* email
* dateOfBirth
* isFirstGp
* wantsSmokingAdvice
* person of parental responsibilityRelationship
* person of parental responsibilityTitle
* person of parental responsibilityFirstName
* person of parental responsibilityLastName
* person of parental responsibilityDateOfBirth
* person of parental responsibilityContactNumber
* person of parental responsibilityEmail

**Non-Personal Data Points used to provide the patient with the best service**

* id (identifier allocated by Healthtech-1)
* gpCode
* gpName
* namedGp
* gpWebsite
* gpEmail
* gpAppointmentsUrl
* createdAt
* registrationReason
* satisfaction
* medicalSatisfaction
* contactConsent
* registrationFor
* hasMobileNumber
* withinPracticeCatchment

**These data / meta-data points in customer.io are internal only, and help us understand where a patient is in their registration journey.**

* updatedAt
* registrationType
* registrationModifiers
* internalStatus
* lastCompletePage
* internalStatusMedicalForm
* lastCompleteMedicalPage

**Twilio:**

* First name
* Mobile number
* GP Practice
* Usual GP

**Postmark:**

* Patient last name
* Patient DOB
* Patient Title
* Passover to practice reason - (automated admin note created by Healthtech-1 team, with no sensitive information included)

#

# Appendix E: List of variables and the questions on the form.

|  |  |
| --- | --- |
| catchmentPostcode | First let's check we serve your address. What's the patient's postcode? |
| title | Your title |
| firstName | Your first name |
| middleName | Your middle name(s) |
| lastName | Your last name |
| email | Your email address |
| hasMobileNumber | n/a |
| mobileNumber | Your mobile number |
| hasHomeNumber | n/a |
| homeNumber | Your home number |
| registrationFor | Who are you registering for? |
| registrationReason | Why are you registering today? |
| representativeTitle | What's your title? |
| representativeFirstName | What's your first name? |
| representativeLastName | What's your last name? |
| representativeGender |  |
| representativeEmail | What's your email address? |
| representativeContactNumber | What's your contact number? |
| representativeRelationship | What's your relationship to the patient? |
| nhsNumber | What's your English NHS number? |
| gender | How would you describe your gender identity? |
| isSameSexAtBirth | Is your gender identity the same as the sex you were registered at birth? |
| sexualOrientation | What's your sexual orientation? |
| religion | Your religion? |
| dateOfBirth | Whats your date of birth? |
| ethnicity | What's your ethnicity? |
| comingBackFromLivingAbroad | Are you are coming back from living abroad? |
| lastLeaveUk | When did you leave the UK? |
| lastReturnUk | When did you return to the UK? |
| ukBorn | Were you born in England? |
| birthCountry | Where were you born? |
| firstLiveUk | When did you first come to live in England? |
| needsInterpreter | Do you need an interpreter? |
| interpreterLanguage | Which language do you need translation for? |
| isArmedForces | Have you been registered with an Armed Forces GP before? |
| armedForcesRole | What were you registered as? |
| enlistmentDate | What is your enlistment date? |
| attendsEducationalInstitution | Do you attend an educational institution? |
| educationalInstitutionType | What kind of institution is it? |
| educationalInstitution | What's the name of it? |
| hasSiblingWithSameDateOfBirth | Is the child one of multiple siblings with the same date of birth? |
| isFostered | Is the patient a fostered child? |
| hasSocialWorker | Do they have a social worker? |
| socialWorkerName | What is the social worker's full name? |
| socialWorkerContactNumber | The social worker's contact number |
| socialWorkerEmail | The social worker's email address |
| roomNumber | Please type the postcode of your address |
| addressLine1 | Please type the postcode of your address |
| addressLine2 | Please type the postcode of your address |
| addressLine3 | Please type the postcode of your address |
| postTown | Please type the postcode of your address |
| county | Please type the postcode of your address |
| dependantLocality | Please type the postcode of your address |
| ward | Please type the postcode of your address |
| postcode | Please type the postcode of your address |
| livesInCareOrNursingHome | Do you live in a residential care home or a nursing home? |
| summaryCareRecordConsent | Would you like to share a summary of your GP care record (SCR) with authorised care professionals? For example, NHS 111, 999 and Accident & Emergency departments. |
| childRegWithoutPersonOfParentalResponsibility | n/a |
| livesWithpersonOfParentalResponsibility | Does the child also live with the person with parental responsibility? |
| personOfParentalResponsibilityTitle | What's their title? |
| personOfParentalResponsibilityFirstName | What's their first name? |
| personOfParentalResponsibilityLastName | What's their last name? |
| personOfParentalResponsibilityGender | What's their gender? |
| personOfParentalResponsibilityDateOfBirth | What's their date of birth? |
| personOfParentalResponsibilityContactNumber | What's their contact number? |
| personOfParentalResponsibilityEmail | What's their email address? |
| personOfParentalResponsibilityRelationship | What's their relationship to the child? |
| personOfParentalResponsibilityIsPatientAlready | Is the person with parental responsibility already registered at {gpCode}? |
| personOfParentalResponsibilityRoomNumber | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityAddressLine1 | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityAddressLine2 | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityAddressLine3 | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityDependantLocality | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityWard | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityPostTown | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityCounty | What's the postcode of the person with parental responsibility's address? |
| personOfParentalResponsibilityPostcode | What's the postcode of the person with parental responsibility's address? |
| emergencyContactTitle | The next of kin's title |
| emergencyContactFirstName | The next of kin's first name |
| emergencyContactLastName | The next of kin's last name |
| emergencyContactGender | Their gender |
| emergencyContactEmail | Their email address |
| emergencyContactContactNumber | Their contact number |
| emergencyContactRelationship | What's the next of kin's relationship to you? |
| emergencyContactStartedPermissionOfCare | When did permission of care start? |
| emergencyContactLivesWithPatient | Do they live with you? |
| emergencyContactCanDiscussMedicalRecords | In the case of an emergency, can we discuss your medical record with them? |
| emergencyContactIsCarer | Are they your carer? |
| emergencyContactIsPatientAlready | Are they a patient with us already? |
| hasHadPreviousNames | Have you had other first or last names in the past? |
| previousFirstNames | Previous first name(s): |
| previousLastNames | Previous last name(s): |
| hasMoved | Have you lived at an address in the UK that is different to your current address? |
| previousAddressLine1 | Please type the postcode of your previous address: |
| previousAddressLine2 | Please type the postcode of your previous address: |
| previousAddressLine3 | Please type the postcode of your previous address: |
| previousCounty | Please type the postcode of your previous address: |
| previousDependantLocality | Please type the postcode of your previous address: |
| previousWard | Please type the postcode of your previous address: |
| previousPostTown | Please type the postcode of your previous address: |
| previousPostcode | Please type the postcode of your previous address: |
| isFirstGp | Have you ever had a GP in England before? |
| previousGpCode | Who was your previous GP practice? |
| previousGpName | Who was your previous GP practice? |
| keepPharmacy | Would you like to keep your current pharmacy? |
| preferredContactMethod | What's the best way to contact you when it comes to your medical circumstances? |
| contactConsent | Can we contact you about updates at the practice? |
| satisfaction | How happy are you with this registration process? |
| satisfactionFeedback | Why did you give that score? |
| has\_repeatMedications | Does the patient have any repeat prescription medication? |
| repeatMedications | Does the patient have any repeat prescription medication? |
| longTermConditions | Does the patient have any of the following long term conditions? |
| wantsBBVScreening | Would the patient like a blood borne virus screening test? |
| hasDisabilities | Do you have any disabilities? |
| disabilityDescription | Please provide more details about your disabilities |
| weightKg | How tall are you in centimetres? |
| heightCm | How much do you weigh in kilograms? |
| hasAllergies | Do you have any allergies? |
| allergies | What's the allergy? / How does this allergy affect you? |
| exerciseFrequency | How much exercise do you do? |
| smokingStatus | What's your smoking status? |
| dailySmokingFrequency | How many cigarettes did you or the patient smoke per day? An estimate is fine |
| wantsSmokingAdvice | Would you like free smoking advice and support? |
| alcoholStatus | Do you drink alcohol? |
| alcoholOverGuidelineFrequency | In the last year, how often have you had 8 (for men) / 6 (for women) or more units of alcohol on a single occasion? |
| alcoholFailedToActNormally | In the last year, how often have you failed to do what was normally expected of you because of drinking? |
| alcoholLostMemory | In the last year, how often have you forgotten what happened because you had been drinking? |
| alcoholConcernFromOthers | In the last year, has a relative, friend, doctor or other health worker been concerned about your drinking or suggested that you cut down? |
| offeredHIVTest | Would the patient like to be tested for HIV? |
| wantsHIVTest | Would the patient like to be tested for HIV? |
| wantsChlamydiaTest | Would the patient like to be tested for Chlamydia? |
| medicalSatisfaction | Are you happy with this medical survey? |
| ppgConsent | Would you like to be part of our Patient Participation Group? |

# Appendix F: System Requirements

For a Healthcare Organisation to enable our Sanny software to complete registrations, they need to have:

* EMIS Web or SystmOne installed on a valid copy of Windows 10 (or over)
* Access to the internet and a secure email inbox
* The ability to share an online form link with their patients

# Appendix G: Automation Smartcard RBAC

The following RBAC positions have been reviewed and approved for Healthtech-1 use by NHSE National RA, Cyber Operations and PDS teams.

EMIS:

|  |  |  |
| --- | --- | --- |
| RBAC Code | Type | Description |
| R8008 | baseline | Admin/Clinical Support Access Role |
| B8029 | additional | Manage Detailed Health Records |
| B8017 | additional | Manage Patient Administration |
| B0264 | additional | Access CSA (Perform Patient Trace) |
| B8009 | additional | Register Patient with Primary Care Provider on PDS |
| B0830 | additional | Perform Patient Demographics |
| B0825 | additional | Amend Patient Demographics |
| B0994 | additional | Manage Ad Hoc Reports (Local) |
| B8020 | additional | Perform Test/Investigation Requests |
| B0020 | additional | Control Consent Status  |

SystmOne:

|  |  |  |
| --- | --- | --- |
| RBAC Code | Type | Description |
| R8008 | baseline | Admin/Clinical Support Access Role |
| B8029 | additional | Manage Detailed Health Records |
| B8017 | additional | Manage Patient Administration |
| B0264 | additional | Access CSA (Perform Patient Trace) |
| B8009 | additional | Register Patient with Primary Care Provider on PDS |
| B0830 | additional | Perform Patient Demographics |
| B0825 | additional | Amend Patient Demographics |
| B0994 | additional | Manage Ad Hoc Reports (Local) |
| B0435 | additional | Manage Tests |
| B0020 | additional | Control Consent Status  |
| B0540 | additional | Execute Reports and Queries |

1. Anonymous information is 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 [↑](#footnote-ref-1)
2. 'Controller' means alone or jointly with others, the organisation that determines the purposes and means of the processing of personal data – for example, this is the case where an organisation is obliged by law to carry out a specific function [↑](#footnote-ref-2)
3. ‘Processor’ means alone or jointly with others, the organisation is processing personal data under the instruction of a Controller and **does not** determine the purposes and means of the processing of personal data [↑](#footnote-ref-3)
4. The [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/) is a self-assessment tool provided by NHS Digital to assess compliance to the 10 National Data Guardian Security Standards. [↑](#footnote-ref-4)
5. ‘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. [↑](#footnote-ref-5)
6. See [NHS Confidentiality Code of Practice](https://www.digital.nhs.uk/cop) Annex C for guidance on where consent should be gained. NHS Act 2006 s251 approval is authorised by the National Information Governance Board Ethics and Confidentiality Committee and a reference number should be provided

 [↑](#footnote-ref-6)
7. Direct marketing is “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals” - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations

 [↑](#footnote-ref-7)
8. Examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention

 [↑](#footnote-ref-8)
9. 'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements [↑](#footnote-ref-9)