Rapid Health Data Protection Pack for GP Practices

This pack provides information on a range of Rapid Health services.

Practices need to extract the elements relevant to their usage of Rapid Health.

Restricted circulation: This document includes information that is confidential and not for publication.

Rapid Health, 86-90 Paul Street, London, EC2A 4NE

CONTENTS

1. Introduction

This document is an information pack to assist GP Practices to complete their Data Protection Impact Assessment (DPIA) for the elements of Rapid Heath that they use. It is not a DPIA but structured similarly to help data controllers to complete theirs.

GP Practices are the data controller for personal data relating to patients and health care professionals that use Rapid Health; Rapid Health is the data processor on their behalf.

The Rapid Health services include:

Smart Triage	A patient-facing service that supports: • administrative requests • medical requests for 16+ • self-help (a patient-facing symptom search with links to NHS information) Practices have an associated **Smart Inbox** to allow them to manage the requests received. There is extensive configuration flexibility so that practices may configure Smart Triage according to local circumstances; this allows practices to determine what level of self-service should be available to patients, and whether patients without an email address on the principal clinical system may self-book an appointment.
Patient Direct Booking	A practice facility to create a generic appointment link to send to a patient of any age.
Smart Direct Booking	A patient-facing service where patients select an appointment type and may book it if their answers match the appointment criteria

In this and related documents the term “Smart Practice” may be used from time to time to group these elements of the Rapid Health platform.

2. Overview

High level description of the Initiative:

Rapid Health comprises software designed to support appointment planning, prioritisation and booking. It supports decisions and can advance from one step to the next based on the data the patient inputs which are validated against the rules configured for the practice for that action type and context.

The Rapid Health solution is defined as automated workflow software as it uses set criteria defined by clinicians for medical requests and appointments, and by administrators for administrative activities. While it may be classified as Artificial Intelligence (AI), no machine learning technology or large language model is used and it does not perform tasks normally requiring human intelligence, such as clinical intervention.

Practices may use all or part of the Rapid Health product suite. Additionally, there is extensive configuration so that practices may use the product in the way that works for their operating model.

What is in scope and excluded from scope?

The information in this document covers Rapid Health's Smart Practice suite. It includes:

- the end-to-end patient experience from entry of patient information to its presentation to the Practice.
- the management of information in the Smart Inbox.
- the booking of appointments associated with patient requests.

It excludes the processing of personal information by clinicians and its storage in the principal clinical system where Rapid Health is not used to directly update the patient record.

Medical Request	Allows a patient to request medical advice. Information is sent securely to the Practice and is saved directly to the patient record by Rapid Health or by the Practice. Depending on the problem and patient's answers, the patient information is sent to the GP linked to a self-booked appointment, or sent to the Smart Inbox for practice follow up. The management of this is assessed through clinical safety oversight and driven by Practice configuration options.
Admin Request	Allows a patient to make administrative requests such as to update personal details, request a sick note, request test results, submit a referral, request repeat prescriptions, or register for the electronic prescription service. This may lead to an appointment at the discretion of the Practice. Practices configure what options are available to patients.
Patient Direct Booking	Allows a patient to book an appointment in response to an SMS or email invitation from the practice.
Smart Direct Booking	Allows a patient to book a specific appointment type via the Practice website such as for a shingles vaccine, a smear test, or for a First Contact Physiotherapy assessment with their GP Practice or a GP Practice offering the service across the Primary Care Network.
Manage Appointment	Allows a patient to cancel or modify an existing appointment when the appointment has been booked through Rapid Health. The patient uses the link in their confirmation communication to cancel or change the appointment. Personal details are required to validate the patient.

Rationale as to why a DPIA is required by the GP Practice:

It relates to a new software product to the GP Practice which will process patient personal and sensitive health data.

3. Consultation

Input of data subjects

There is a strong, recent precedent for services such as Rapid Health's. The use of online services is already well-established in the UK and widely used across GP Practices. Government is directing GP Practices to harness technology to help them to spread finite resources more efficiently.

Rapid Health Smart Triage and Rapid Health Smart Direct Booking provide a text-based clinical consultation service which guides patients through an automated workflow based on the data the patient inputs to describe their symptoms or administrative need. Rapid Health recommends appropriate next steps which may include arranging a GP appointment, self-care advice or signposting to other services (eg NHS111, pharmacies etc.) depending on the GP Practice configuration. Depending on the outcome of the patient interaction, practices will get the patient requests and any associated booked appointment*.

Online services provide opportunities for patients to engage with their GP Practices remotely and at a time that is convenient. The use of automated clinical workflows can help GP Practices to optimise contact with clinicians, helping to route the right patients to the right clinician at the right time. The services can reduce the burden on clinical and administrative staff while helping to increase consistency of information capture and improve the prioritisation of care. Rapid Health relied on research and the widespread use of such services and government/NHS direction in these matters, so did not consult patients on the concept.

A Health Innovation evaluation of Rapid Health undertaken by Unity Insights found that significant benefit accrued to patients following the adoption of Rapid Health by their practice.

*Practices will not know if a patient a) cancels a request, ie does not complete it, or b) is not allowed to complete it, due to ineligibility. Patients are warned that the GP will not get their request if they cancel.

GP Practices	Supporting their requirement to complete a DPIA as data controllers To provide support for GP Practices during implementation. GP Practices to implement procedures for staff in the use of the Rapid Health software.

4. Supplier compliance

Supplier	Compliance credentials	Role/compliance note
Rapid Health ODS: 8KG49	DSPT (2024-25) – Standards met ICO Registration – ZA620101 Cyber Essentials certificate: 862698d4-ece6-45ef-b3f3-593764bdc609, 3/11/2025 There will be appropriate agreements in place to support GDPR Articles 24 and 28.	Principal data processor. You should also be aware that Rapid Health, as a normal part of its operations, continually updates its services and technology as appropriate.

Supplier	Compliance credentials	Role/compliance note
8foldGovernance (IG consultancy) ODS: 8KG85	DSPT (2024-2025) – Standards met Cyber Essentials Plus – 34d2766d-26f9-40b4-8c8f-97d6ba3d9793, 13/10/2025	Rapid Health uses 8fold Governance for Information Governance as a Service and for Clinical Safety as a Service. 8fold Governance does not normally need to process any Smart Triage personal data except in the event of a data breach or clinical safety incident if there is a reason to do so.
Amazon Web Services (**AWS**) ODS: 8JX11	Data Processor and Storage Provider DSPT (2024-25) – Standards exceeded ISO/IEC 27001:2022, 13/08/2025 Cyber Essentials Plus – 0e793249-f3de-4efa-8f53-250eeae277ea, 21/03/2025	All Rapid Health data is hosted in AWS Cloud eu-west-2 (London, UK). All information to Rapid Health services and databases is encrypted in transit and at rest to TLS 1.3.
Atlassian Cloud ODS: n/a	Data Processor for Rapid Health internal operational support ticket management ISO 27001:2024-01 Certificate no. 13080125, 25/07/2025 SOC 2 Type II, 25/11/2024	All technical work at Rapid Health is managed through Jira/Atlassian Suite, to ensure full traceability from analysis through to deployment of any change. When Rapid Health needs to carry out technical analysis following a support enquiry, Rapid Health uses the integration within Freshdesk (the support ticketing system) to raise a ticket in Jira, which is part of Atlassian Suite. As the ticket is linked to Freshdesk, correspondence in Freshdesk is included within the Atlassian audit trail. Additionally, Rapid Health uses Confluence for documentation. The Rapid Health data residency for Atlassian Cloud is set to the UK.

Supplier	**Compliance credentials**	**Role/compliance note**
EMIS Health Egton Medical Information Systems Limited ODS: YGM06	DSPT (2024-25) – Standards exceeded Cyber Essentials Plus – dc0f68d0-958d-42f3-8116-ad8ddc3fbe51, 23/04/2025 ISO/IEC 27001 Information Security Management Certificate Number - IS 75688 (LC24) ISO 9001:2015 Quality Management - Certificate Number - FS 68475 ISO 22301 - Certificate Number - BCMS 700899	Rapid Health reads and writes to patient records held on EMIS for practices that use it as their principal clinical system. Rapid Health completes bi-annual reassurance with EMIS to confirm that Rapid Health meets required standards for using EMIS APIs and manages information governance and clinical safety issues. The most recent reassurance was May 2024.
Freshworks Inc ODS: n/a	Data Processor Cyber Essentials Plus – 28373f55-b2f5-491d-a7b1-ac828cc7e19e, 06/02/2025 SOC 2 Type 2 ISO/IEC 27001:2022 Certificate no IS 666070, effective 01/09/2025	Rapid Health uses its Freshdesk support desk service which integrates with Atlassian Suite and Rapid Health Smart Triage. GP practices may use a Help button in the Smart Inbox to raise a ticket in Freshdesk for Rapid Health support. The integration provides information about the practice and a request reference if the practice query is for a specific request. The reference identifier allows the Rapid Health technical team to investigate audit logs precisely. The Rapid Health data residency for Freshworks is in the EU.
Health and Social Care Network (**HSCN**) – NHS England, formerly NHS Digital X26 ODS: X24	Data Processor and Storage Provider X24 NHS DSPT (2024-25) – Standards met	Data from Rapid Health is transferred to the GP Practice via the HSCN which provides a secure data storage and processing service. Information is encrypted in transit and at rest. This is the process that allows suppliers to integrate their system with any principal clinical system through an interface mechanism. Rapid Health is obliged by the NHS to utilise the HSCN for communications with GP Practices.

Supplier	Compliance credentials	Role/compliance note
NHS England – formerly NHS Digital X26 ODS: X24	Data Controller and Storage Provider X24 NHS DSPT (2024-25) – Standards met	Patients may provide their credentials for using Rapid Health for a specific GP practice via NHS login (from the GP practice website or via NHS App). Privacy statement: https://access.login.nhs.uk/privacy
The Phoenix Partnership (Leeds) Ltd, provider of **SystmOne** (TPP) ODS: YGM24	DSPT (2024-25) – Standards exceeded Cyber Essentials Plus – e13d0fca-b753-4994-95de-7dcbd58fa028, 13/05/2025	Rapid Health reads and writes to patient records held on SystmOne for practices using it as their principal clinical system. Rapid Health completed assurance with TPP and the NHS IM1 team to confirm that Rapid Health meets required standards for using SystmOne APIs and manages information governance and clinical safety issues. Initial assurance completed 28/09/2023.

5. Description of processing

Data flow map(s):

See Appendix E – Data flow map

Description of the proposed processing operations:

Practices may use all or part of the Rapid Health product:

1. **Self Help:** (patient-initiated)
   a. Patients use this service anonymously. No data relating to an individual's use is retained, ie no IP address or cookies.
   b. They enter a symptom or complaint and if it's matched, the associated NHS information is shown.
2. **Patient Direct Booking**: (practice-initiated)
   a. Rapid Health allows the practice to generate a link for a specific or generic appointment type. No personal data is associated with this link unless the appointment specifies practice personnel.
   b. Links are sent to patients via systems external to Rapid Health, such as Outlook or accuRx; any associated content is not known to Rapid Health.
   c. When a patient clicks on an appointment link, they are authenticated against the principal clinical system before they can book an appointment. Rapid Health updates the Practice appointment book if a successful booking is made.
   d. Patient Direct Booking links may be used for patients of any age.
3. **Smart Direct Booking**: (patient-initiated)
   a. Patients can use the practice website to book a specific appointment type such as a shingles vaccine, a smear test, or for a First Contact Physiotherapy assessment.
   b. The patient is authenticated and asked questions to check their eligibility for the appointment.

c. Depending on the rules set for the appointment, the patient is:
   i. allowed to book in, or
   ii. advised they are not eligible, or
   iii. signposted to the practice as they may need a different appointment type, or
   iv. signposted to an alternative provider, or
   v. asked to confirm to send their request to the practice for follow-up.

4. **Smart Triage**:

a. Patients go to a Rapid Health menu within the practice website. From there they can choose medical or administrative requests, or access self-help which links to NHS help.

b. **Medical request** enquiries are assessed for urgency against rules for red and amber flags and other potentially urgent or serious symptoms. The only free text they enter is their symptom/ problem search. They are graded into an urgency category. Depending on the practice set-up:

   i. Patients may book into an appointment of an urgency that aligns with the symptoms entered for the medical request and their answers are saved into their record.

   ii. Patient requests that are not offered an appointment are sent to a Smart Inbox for review and follow-up by clinicians and then saved to the patient record; the clinician may invite the patient to self-book an appropriate appointment.

   iii. Practices may choose to review the request notes for patients who have been able to book into an appointment as a quality control before saving the notes to the record.

c. **Admin request** enquiries for needs such as fit notes, test results, prescription renewals or questions to the practice may be submitted.

These requests are routed to an administrative section of the Smart Inbox where GP Practice administrators process them and may save them to the patient record. They may invite the patient to self-book an appointment with an administrator or clinician, depending on the Practice's assessment of the patient request.

A patient must take an affirmative action for the practice to receive their request.

Types of personal data: (See Appendix D for the full data collection matrix

GP Practice Staff:

- First and Last Name
- Organisation Details
- NHS Email Address
- Username and Password
- IP Address

Patients:

- First and Last Name
- Middle Name (if entered)
- Address
- Post Code
- Phone Number(s)
- Email Address
- Date of Birth
- Sex at birth
- Health
- NHS number (used for internal processing – not entered by the patient)
- Principal clinical system identifier (used for internal processing – not entered by the patient)
- Rapid Health reference – a unique reference generated for a patient request
- Message Content – administrative request content

If a third party’s contact details are given by a patient, these are not saved to the record by Rapid Health but made available to the practice staff in the Smart Inbox for the purpose of request processing except where the “Best number to call on” is not the patient’s: this number is stored with any appointment details.

Types of data subject:

The primary data subjects are UK patients aged 16 or over registered with GP Practices. These data subjects use the patient-facing application.

Rapid Health is designed for use by the patient. If a patient uses the support of a third party, they may enter this person’s phone number as the best number to reach them on, and provide an explanation about why the practice should call this person. This data is not saved to the principal clinical system, and the practice must use its discretion.

Practices may at their discretion invite children younger than 16 to an appointment using the Patient Direct Booking facility. This is an appointment booking only, ie no other information is collected.

Professional users include GP Practice and Primary Care Network staff whose access is authenticated. They use the practice-facing Smart Inbox application.

Sources of the personal data:

Patients
Practice staff

Length and frequency of processing:

As required by the patient

Processing volumes:

The volumes are dependent on practice policy and demographics. They depend on how often a patient chooses to engage with the Rapid Health services; note that Patient Direct Booking is practice-led, but the other elements are patient-initiated.

Data minimisation:

Smart Triage uses minimal identifiers from the patient to validate their details prior to being able to access the services.

The patient does not need to enter their NHS number – this is retrieved by Rapid Health and associated with the patient session to ensure that the patient match is efficient and accurate. The NHS number is also required to book patients into other organisations’ appointment books, eg for resources shared across a Primary Care Network PCN or General Practice Federation. This meets Personal Demographics Service PDS and GP Connect API requirements.

Smart Direct Booking and Smart Triage medical requests use patient questionnaires that contain pre-set responses so the minimal amount of information is required and may be used to direct the patient to the appropriate service. Some questionnaires offer the patient supplementary, optional questions to provide further information, and these are answered at the discretion of the patient, eg a PHQ9 questionnaire.

Smart Triage admin requests allow free text. The free text boxes have been kept short to discourage unnecessarily extensive information, but the content is at the patient’s discretion. All admin forms make clear that they should not be used for urgent medical requests.

Patient data is retained in the GP Practice inbox until its inbox retention period has been completed. See Appendix C – Data retention for specific retention periods and approach.

6. Basis of processing

Lawful processing

Necessity and proportionality assessment (assessment of the necessity and proportionality of the processing operations in relation to the purpose(s)):

Purpose limitation:

The information provided by the patient is used by Rapid Health for the purposes of prioritising their healthcare when seeking medical advice or submitting requests and enquiries for sick notes, test results or prescription renewals.

Lawfulness of processing

The lawful basis of healthcare staff using Rapid Health for communicating with patients is understood to be:

6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'.

9(2)(h) '…medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems…'.

Automated decision-making

The Rapid Health Smart Triage system does not comprise automated decision-making as defined by the UK GDPR.

Its 'decisions' do not meet the threshold of producing legal effects concerning individuals or similarly significantly affecting them in a way that mandates the requirements of the additional safeguards outlined in Article 22: each patient request is assessed against clinical criteria and appointment availability, with the option for patients to contact the practice directly if no self-booking is available for their request.

Rapid Health

Rapid Health does not require the patient to download an app to use its services. Patients access the service via a browser on their smart device/PC.

Communications between the patient and healthcare professional are encrypted in transit via HTTPS and responses are encrypted at rest.

A separate document that details how patient authentication is carried out is available on request.

Data Protection Principles and Assessment of Compliance	
Principle	**Assessment of Compliance**
GDPR Principle A: Processed lawfully, fairly and in a transparent manner in relation to individuals (*lawfulness, fairness and transparency***)**	Patients' personal data is processed under the lawful basis of the provision of healthcare.
GDPR Principle B: Personal data shall be collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (*purpose limitation*)**	Patients must provide identifying information that is matched by the Smart Triage against the Practice EPR (EMIS / SystmOne) system to ensure the patient has an active registration at the practice. The patient provides this directly or via NHS login. Patients them complete a series of questions which directs them to options depending on the information provided.
GDPR Principle C: Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*data minimisation***)**	Drop down response fields are used to limit the information provided so that it remains relevant to the query. Where the patient submits an Admin Form request there is a limited entry capacity free text field.
GDPR Principle D: Personal Data shall be accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (*accuracy***)**	The information provided by the patient will give the healthcare professional an up-to-date view of the patient's circumstances and this can be added into the patient's medical record to ensure an accurate and up to date record is maintained.
GDPR Principle E: Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisation measures required by the GDPR in order to safeguard the rights and freedoms of individuals (*storage limitation***)**	Patient information is not retained on the Smart Triage platform but retained in the patient's registered GP Practice records.
GDPR Principle F: Personal Data shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures (*integrity and confidentiality***)**	Rapid Health has completed the NHS Data Security and Protection Toolkit (8KG49) – 23/24 Standards Met. Rapid Health's sub processors operate based on Article 28 GDPR compliant agreements. Rapid Health data is encrypted at rest using industry-standard AES-256 encryption algorithm and in transit via HTTPS to TLS 1.3.

Rights and freedoms assessment (assessment of the risks to the rights and freedoms of the data subjects):

GP Practices are the data controllers for patient information and as such will retain responsibility for responding to data subjects' requests in line with their local policies and procedures.

Fair processing:

The patient is provided with a privacy notice 'how we use your information' prior to entering their personal details to access the Smart Triage services.

7. Purpose(s) of processing; benefits and risks

Purpose(s) of processing

Rapid Health's Smart Triage helps GP Practices to prioritise the care of patients seeking medical advice. It also facilitates patient administrative requests and enquiries. Patients can submit a request and/or self-book an appointment at a time that is convenient to them.

By reducing the administrative burden on practices to manage the capturing of patient requests, more time is available to carry out other work. This also helps patients who can't join the 8am phone queue.

While not everyone has the ability or access to online services, freeing up practice staff from those who means there is capacity to support those without online access.

A description of the services is provided in the Overview section, and risks are set out below.

8. Security of processing

Practical safeguards:

Rapid Health complies with the NHS Data Security and Protection Toolkit 23-24.

Identity and access management arrangements:

- GP Practice Healthcare staff access is authenticated using role-based access controls
  - The GP Practice IT Team identifies the list of users, and their NHS email addresses.
  - Rapid Health emails each individual user to their NHS email address and they complete account set up for the Smart Triage Practice Inbox where healthcare staff can view all incoming requests. Healthcare staff must log in using their NHS email address to use it.
- Patient's access is authenticated.
  - Patients access Smart Triage via their own device. They do not need to login but must provide patient information that is matched by Smart Triage against the GP Practice EPR [EMIS/SystmOne]. Interactions with a patient are confirmed by email or SMS to the email/SMS details held on the GP Practice system to ensure that any attempt to impersonate the patient will be alerted to the patient. A separate document that details how patient authentication is carried out is available on request. See **Error! Reference source not found.** for further information.
- Rapid Health staff access is authenticated and authorised using role-based access controls
  - Access to the data is limited to authorised personnel when strictly necessary (for example in the event of incident resolution).
  - Systems access is regularly audited.

- The Smart Inbox presents patient requests to the Practice and provides the Practice with tools to manage the requests. Each request has an associated Activity Log which shows the history of how the Practice is managing the request, ie any views of the request, who the request has been assigned to, who has assigned the request, and who has carried out actions in relation to a request, such as inviting the patient to an appointment.

Security measures:

Rapid Health as data processor retains data on secure servers based in England on the AWS infrastructure. The data is encrypted in transit and at rest and is stored on encrypted disks. Rapid Health's Smart Triage software is subject to annual penetration testing.

9. Data quality

Assessment of quality:

In Smart Direct Booking and Smart Triage medical requests, once the patient has been authenticated the only free text input is numeric, eg how many months since the first shingles vaccine dose. All other data collection uses radio buttons, dropdowns and multichoice field types. This is to ensure that the patient is supported to give a complete history and that the histories taken from patients will be consistent and may be interpreted consistently. Some questions also allow for 'None of the above' or 'I am not sure' depending on the question, to avoid patients being forced into a Yes/No answer where the answer may be that they don't know.

Free text fields are used when a patient wishes to use the Smart Triage admin request service, eg to request fit notes or send a general enquiry to the practice. Word counts are applied to encourage succinct presentation of the information and to help patients to understand that they are not required to provide extensive information. The word counts are context-specific to enable sufficient information to be provided.

Patients must take affirmative action to submit a request or book an appointment. There is no concept of an incomplete shopping cart where a Practice can view incomplete requests.

GP Practices receive information in their 'Smart Inbox' which requires them to act, such as saving the information into the patient record. Where any data quality issues are identified these can be raised with the patient and rectified at the time. An Activity Log is available for the Practice to view so that they can see the history of each request.

Answers provided by patients using the Smart Direct Booking service are saved to the patient record so that they are available for the appointment that they have booked. In the event no appointment is available and a Practice requires that the patient is signposted without updating their record, this is carried out, but the default is to ensure the patient information is captured and either presented for action in the Smart Inbox or at the time of the appointment where the patient has been able to book one.

It is recognised that a patient seeking an appointment via Smart Triage or Smart Direct Booking may over-state or under-state a situation, either to 'game' the system or out of humility. The question strategy attempts to collect sufficient information to counter this, but if a patient does not pay attention to the questions, has limited English, does not understand a question or is not aware of symptoms, then the presented information may not be a full reflection of the situation for the patient. The information captured from and for the patient is an input to a subsequent evaluation by the Practice and does not replace the role of the Practice in assessing the information.

The Smart Inbox has two easy ways for Practices to provide feedback to Rapid Health to support ongoing improvement:

1. there is an "Improve Logic" function for each patient medical request, and
2. a Help button which allows the Practice to send comments directly to Rapid Health without needing to log in to a separate system. When they use the Help button this automatically captures the reference for the patient request if the button was used for a specific request. This helps with data accuracy and helps to discourage practices from providing more patient personal data.

10. Arrangements to address individual rights

Each GP Practice will have their own processes in place regarding arrangements to address individual's rights.

Right to be Informed

Patients who choose to use Rapid Health are provided with a privacy notice at the point they are asked to provide their personal data to ensure all usage of their personal data is in line with their reasonable expectations.

Right to Rectification: (where applicable)

Rapid Health is transactional. It captures information directly from the patient and reflects a point in time, ie this information is not maintained by Rapid Health but used to facilitate subsequent action by the GP Practice. If the patient enters any information erroneously, the record captured by Rapid Health can be altered by the Practice but not by Rapid Health. It is expected that a clinician consulting with the patient will re-confirm information – Rapid Health's role is to aid the Practice with appointment prioritisation and booking, but not to diagnose. The GP Practice will rectify information on the patient record or will take updated information into account when actioning the request.

Right to Erasure: (where applicable)

GP Practice patient records are considered a medico-legal record which are maintained in the exercise of official duty vested in them as data controllers and must be retained for the establishment, exercise or defence of legal claims.

Any request to comply with the qualified right to erasure will be considered on a case-by-case basis but is likely to be refused with data remaining on the GP Practice system until the full and defined retention period has been reached.

11. Retention and disposal

Smart Direct Booking

Patient questionnaire data is saved to the patient record when the patient books their appointment.

Depending on the nature of the appointment, a patient's answers are not retained if they are not eligible for the appointment, for example, if a male patient seeks the whooping cough vaccine, he will be advised he's ineligible and will be presented with the NHS eligibility criteria. His answers to the questionnaire are not retained and nor is the fact that he completed the questionnaire.

Where a patient may need medical attention despite being unsuitable for an appointment (eg for an FCP appointment) their completed questionnaire will be provided to the practice Smart Inbox for their attention unless otherwise requested by the practice. It is always the patient choice to submit the request.

Requests routed to the Smart Inbox are managed in the same way as Smart Triage consultations (see below).

Smart Triage:

Smart Triage information provided by the patient is transferred securely to their GP Practice Smart Inbox for Practice staff to action if required, ie some requests have already been actioned and the information will be reviewed at the patient appointment.

The request information may be updated automatically into the GP Practice principal clinical system if the GP Practice has this feature enabled and the criteria are satisfied; otherwise manual intervention will be required by GP Practice staff. Each request in the Smart Inbox has a reference ID.

Patient data is retained in the GP Practice Smart Inbox as follows:

- **Medical Requests**: **two (2) weeks** from the date processed by the Practice. Once the two weeks have lapsed the data is no longer available in the GP Practice Smart Inbox. GP Practice staff must ensure that the data is saved to the patient record in a timely manner to ensure the accuracy of the patient record and that any clinical decision making takes place using accurate data.

- **Admin Requests**: **two (2) weeks** from the date processed by the Practice. Once the two weeks have lapsed the data is no longer available in the GP Practice Smart Inbox. GP Practice staff must ensure that the data is saved to the patient record in a timely manner to ensure the accuracy of the patient record and that any clinical decision making takes place using accurate data.

- **Manage Appointments:** saved into the GP Practice system at the point of modification. If the originating request is still in the Smart Inbox, ie has not been archived, it will be updated to show the change to the appointment.

If GP Practice staff identify an issue with patient data from Rapid Health, they raise a ticket from the Smart Inbox, or email to support@rapidhealth.co.uk. The Rapid Health reference is a unique identifier which allows Rapid Health to track down a specific request to assist Rapid Health's audit logs investigation. The Rapid Health reference is saved to EMIS/SystmOne with booked appointments so that practices may refer to any problem without needing to communicate the patient's contact details or NHS number.

Data held for incident management

See Appendix C – Data retention for a diagram showing how data is processed and removed from Smart Inboxes, before being deleted after a period in which data is held for incident management.

Cookies:

Session cookies, also known as transient cookies, are stored in temporary memory and are only available during an active browser session to manage that session. No other cookies are used.

Device type identification and IP addresses:

Rapid Health tracks what devices and operating systems are used by patients. This is to support system design and problem solving. No IP addresses are captured within Rapid Health databases, however services within Rapid Health's wider architecture do record IP addresses temporarily as part of their operation.

12. Actions and Responsibilities

Actions are prioritised into those considered essential to ensure the success of the project (Required) and those recommended to support its success (Recommended), with an associated requirement reason:

Legal	must be completed to ensure compliance with the law.
Assurance	provides assurance to stakeholders and/or provides evidence that best practice is being followed/adopted.
Best Practice	considered best practice and so any deviation from this should be explicitly justified.
Operational	considered necessary to ensure operational success.

Action required – Rapid Health	Actionee	Reason for requirement	Status
DSPT Compliant NHS Data Security and Protection Toolkit (DSPT) submission (version 7) 2024-25, or appropriate assurance statement required from each data processor.	Rapid Health	Legal Assurance Best Practice	Complete
Privacy information signposting Reword 'patient information' to 'how we use your information' on the initial registration screen.	Rapid Health	Legal Assurance Best Practice	Complete
Fair processing notice Fair processing information must be provided to patients at the point their information is collected in Smart Triage. Review wording for accuracy.	Rapid Health	Legal Assurance Operational	Complete
Privacy notice Review, update and publish privacy notices.	Rapid Health	Legal Best Practice Operational	Complete
Training and support for Smart Triage Training and support for staff within GP Practices on how to use Smart Triage.	Rapid Health	Assurance Best Practice Operational	On-going
Routine auditing Routine auditing must be undertaken to ensure appropriate access to their systems and records.	Rapid Health	Assurance Best Practice Operational	On-going
Individual named user accounts Individual (named) email addresses and user accounts must be configured.	Rapid Health	Assurance Best Practice Operational	On-going

Action required – Rapid Health	**Actionee**	**Reason for requirement**	**Status**
User control process A starters, leavers and movers process must be in place to ensure that user access is removed when no longer required.	Rapid Health	Legal Assurance Best Practice Operational	Complete

Action required – GP Practices	Actionee	**Reason for requirement**	Status
Contract for data processing Ensure there is a signed contract in place with the GP Practices or with the GP Federation providing the service on behalf of the GP Practices which includes data processing responsibilities with Rapid Health.	GP Practices / GP Federation GP Practices / Rapid Health	Legal Assurance Best Practice	
Privacy notice Review, update and publish privacy notices.	GP Practices	Legal Best Practice Operational	
Training and support for Smart Triage Training and support for staff within GP Practices on how to use Smart Triage.	GP Practices	Assurance Best Practice Operational	
Fully documented procedures Fully documented procedures must be in place for staff on how Smart Triage software is used.	GP Practices	Best Practice Operational	
Full documented procedures to maintain accurate patient records Fully documented procedures must be in place for GP Federation staff providing the service on behalf of the GP Practices on how to maintain accurate patient records in the registered GP Practice clinical system.	GP Practices	Legal Assurance Best Practice Operational	
Routine auditing Routine auditing must be undertaken to ensure appropriate access to their systems and records.	GP Practices	Assurance Best Practice Operational	
Individual named user accounts Individual (named) email addresses and user accounts must be configured. If a user is to be set up using a non NHS.net email account, the practice must give formal authorisation for this to Rapid Health.	GP Practices	Assurance Best Practice Operational	

Action required – GP Practices	Actionee	**Reason for requirement**	Status
User control process A starters, leavers and movers process must be in place to ensure that user access is removed when no longer required.	GP Practices	Legal Assurance Best Practice Operational	

13. Risk Assessment

Risks identified have been assessed using the following model.

		Impact				
		Trivial	**Minor**	**Moderate**	**Major**	**Extreme**
Probability	**Rare**	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

They have been documented and assessed in detail on the following pages.

Risk 1: what is the identified risk to individuals	**Non-compliance with the law and best practice could result in a failure to safeguard the rights of data subjects (service users).**
Probability: what is the likelihood that the risk will occur	**Likely** - Without the necessary corporate and information governance, it is likely that data sharing will not occur in compliance with the law and best practice and the necessary technical and operational controls will not be identified or implemented to support appropriate sharing of, access to and use of personal data.
Impact: what would the impact be if the risk were to occur	**Major** - The impact of non-compliance with the law and best practice could include a major risk to individuals, data controllers and the ongoing viability of the service through a loss of confidence by data controllers and the public. A breach of law could also result in regulatory action, fines and compensation claims from affected individuals.
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	This impact assessment has assessed the compliance of the operational approach and technical solution.
Additional controls required: (e.g. technical, operational/procedural, etc.)	All actions identified by this impact assessment must be implemented by the GP Practice and Rapid Health to sufficiently mitigate the risk of non-compliance with the law and best practice. This includes the development and implementation of the required policies and procedures and ongoing submission of the NHS DSP Toolkit to evidence the necessary compliance.
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Unlikely**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Moderate**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Likely x Major** reduced to **Unlikely x Moderate = Medium**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	The completion of all actions identified by this document will enable any potential risks posed to data subjects, data controllers and the programme to be sufficiently mitigated.

Risk 2: what is the identified risk to individuals	**Data protection responsibilities are not understood by the contracting parties, ie GP Practices as Data Controllers and Rapid Health as Data Processor and the sub-processors of Rapid Health.**
Probability: what is the likelihood that the risk will occur	**Moderate** Without the necessary contractual controls in place between GP Practices, or a GP Federation acting on behalf of the GP Practices and Rapid Health and Rapid Health and their sub-processors, it is possible that the contract will not be managed in compliance with the law.
Impact: what would the impact be if the risk were to occur	**Major** The contractual rights of the GP Practice and Rapid Health may be infringed.
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	Rapid Health has signed contract in place with their sub processors.
Additional controls required: (e.g. technical, operational/procedural, etc.)	Data Processing Contracts are required.
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Unlikely**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Minor**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Moderate x Major = Medium** reduced to **Unlikely x Minor = Low**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	In advance of a contract being in place, documented authorisation that Rapid Health can provide its service to the GP Practice and that the sub-processors can provide the services to Rapid Health.

Risk 3: what is the identified risk to individuals	**Patient inputs inaccurate data to expedite an appointment.**
Probability: what is the likelihood that the risk will occur	**Moderate** Drop down response fields are in place to limit the information provided so that it remains relevant to the query. A limited character free text field is available for the Admin Forms service.
Impact: what would the impact be if the risk were to occur	**Major** Patients requiring urgent clinical intervention could be delayed. Patients not requiring clinical intervention could be accessing already stretched GP Practice resources.
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	The GP Practice staff should have documented processes in place to alert their Clinical Safety Officer to assist with the accurate assessment of the patient.
Additional controls required: (e.g. technical, operational/procedural, etc.)	The Smart Triage screens advise the patient not to use the software in an emergency or where immediate clinical intervention is required. Smart Direct Booking screens advise patients not to use the software in an emergency or where immediate clinical intervention is required, eg for a First Contact Physiotherapy booking, but not for a vaccination appointment. GP Practices to implement documented procedures for staff on how the Rapid Health software is used.
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Moderate**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Minor**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Moderate x Major = Medium** reduced to **Unlikely x Minor = Low**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	Rapid Health presents the patient with a clear message.

Risk 4: what is the identified risk to individuals	**GP Practice staff not saving patient information from the Smart Inbox to the patient record in a timely manner resulting in patient records omitting patient requests and personal data being kept in the Smart Inbox indefinitely**
Probability: what is the likelihood that the risk will occur	**Likely**
Impact: what would the impact be if the risk were to occur	**Major** If record keeping and records management requirements are not fulfilled, this could result in non-compliance with the law and best practice and result in a major risk to individuals, data controllers and the ongoing viability of the service through a loss of confidence by data controllers and the public. A breach of law could also result in regulatory action, fines and compensation claims from affected individuals.
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	Where self-booking is allowed by practices, the records are updated immediately. GP Practices have operating procedures in line with the NHS Records Management Code of Practice.
Additional controls required: (e.g. technical, operational/procedural, etc.)	GP Practice to implement documented procedures for staff on how the Rapid Health software is to be used.
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Unlikely**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Minor**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Moderate x Major = Medium** reduced to **Unlikely x Minor = Low**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	The existence of operational procedures within GP Practice and incentive to the Practice to maintain current patient records are considered sufficient to reduce both the probability and impact of records management risks.

Risk 5: what is the identified risk to individuals	**Malicious Data Loss**
Probability: what is the likelihood that the risk will occur	**Rare**
Impact: what would the impact be if the risk were to occur	**Major**
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	Rapid Health has the following in place: • Penetration Testing • Role Based Access Controls • Audit Procedures • Scheduled Audits • System Monitoring • Back-up and Recovery process • Training • Policies and procedures • Activity logs showing all actions, who took them (ie system, patient, or Smart Inbox user) and any associated messages are visible on all requests in the Smart Inbox.
Additional controls required: (e.g. technical, operational/procedural, etc.)	None
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Rare**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Minor**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Rare x Major = Medium** reduced to **Rare x Minor = Low**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	The existence of operational procedures within Rapid Health coupled with the technical measures in place are considered sufficient to reduce both the probability and impact of this risk.

Risk 6: what is the identified risk to individuals	**Cyber Attack**
Probability: what is the likelihood that the risk will occur	**Rare**
Impact: what would the impact be if the risk were to occur	**Major**
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	Rapid Health has the following in place: • Patch Management • Firewalls • Anti-Malware • Back-up and Recovery Processes • System Monitoring GP Practices has the following in place: • Procedures to update patient records as soon as possible to ensure accurate and timely information.
Additional controls required: (e.g. technical, operational/procedural, etc.)	None
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Rare**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Minor**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Rare x Major = Medium** reduced to **Rare x Minor = Low**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	The existence of technical and operational procedures within Rapid Health and GP Practices are considered sufficient to reduce both the probability and impact of this risk.

Risk 7: what is the identified risk to individuals	**Inaccurate patient records due to loss of connectivity between the Patient and Rapid Health and Rapid Health and GP Practices.**
Probability: what is the likelihood that the risk will occur	**Rare**
Impact: what would the impact be if the risk were to occur	**Major**
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	Rapid Health has in place: • Patient can telephone the GP Practice • Resilient Infrastructure • Contractual Agreement • Service Level Agreements • Business Continuity Plan
Additional controls required: (e.g. technical, operational/procedural, etc.)	None
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Rare**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Minor**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Rare x Major = Medium** reduced to **Rare x Minor = Low**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	The existence of operational procedures and contractual agreements in place within Rapid Health and the GP Practices coupled with the technical measures in place are considered sufficient to reduce both the probability and impact of this risk.

Risk 8: what is the identified risk to individuals	**Inaccurate patient records held at GP Practices due to manual intervention by the GP Federation providing the service on behalf of the GP Practices**
Probability: what is the likelihood that the risk will occur	**Likely**
Impact: what would the impact be if the risk were to occur	**Major**
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	GP Practices have in place: • Documented procedures for the validation of patient information • Contractual Agreement with GP Federation (as the data processor) providing the service on the GP Practice (as the data controller) behalf
Additional controls required: (e.g. technical, operational/procedural, etc.)	GP Practices to document operational procedures for information relating to their patients to be updated on practice clinical systems and not held on the GP Federation clinical systems.
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Unlikely**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Major**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Likely x Major = Medium** reduced to **Unlikely x Major = Medium**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	This is a temporary arrangement until GP Connect is implemented. This with the existence of operational procedures and contractual agreements in place between the GP Practices and the GP Federation and with Rapid Health and the GP Federation as the GP Federation are providing this service on behalf of the GP Practices. These coupled with the technical measures in place are considered sufficient to reduce both the probability and impact of this risk.

Risk 9: what is the identified risk to individuals	**'unverified' 'self-book' appointments**
Probability: what is the likelihood that the risk will occur	**Likely**
Impact: what would the impact be if the risk were to occur	**Major**
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	• GP Practices have in place documented procedures for the validation of patient information prior to accepting a 'self-book' appointment • Technical controls are in place. Self-book appointments are only permitted where a) the patient has an email address on their record so that a verification message may be sent there, or b) the Practice invites someone directly after satisfying local procedures.
Additional controls required: (e.g. technical, operational/procedural, etc.)	• GP Practices need to use their validation procedures when using the Smart Inbox. • Rapid Health provides a warning message if a request is processed and saved to the record in advance of a subsequent rejection of the patient identity by a Practice administrator, providing details of the requests that need to be reviewed and potentially deleted from the patient record.
Probability: what is the likelihood that the risk will occur with all identified controls in place	**Unlikely**
Impact: what would the impact be if the risk were to occur with all identified controls in place	**Major**
Result: is the risk eliminated, reduced, or accepted?	**Reduced:** **Likely x Major = Medium** reduced to **Unlikely x Major = Medium**
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	The existence of operational procedures coupled with the technical measures in place at GP Practices are considered sufficient to reduce both the probability and impact of this risk.

Risk Assessment and Mitigation

Are there any risks to the **Confidentiality** of personal data? *Confidentiality is defined as unauthorised disclosure of, or access to, personal data.*

None Identified

Are there any risks to the **Integrity** of personal data? *Integrity is defined as unauthorised or accidental alteration of personal data.*

None identified

Are there any risks to the **Availability** of personal data? *Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.*

None identified

Are there any known or immediate technical / IT / Information Security / Cyber Security concerns?

None identified

If the answer is “Yes” to any questions in this section, how are these to be reduced or mitigated?

Once the mitigations are implemented, how would you score remaining risks in the following Risk Assessment? If you consider that there are no remaining risks give a value of 1 for both Likelihood and Severity.

Any risks scoring above 6 will need to be reviewed by either the organisations Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, or IG Manager (depending on availability during the pandemic).

Likelihood *(please tick)*				**Severity** *(please tick)*				
1		Rare	**x**	**1**		Negligible	**=**	4
2	x	Unlikely		**2**	x	Minor		
3		Possible		**3**		Moderate		
4		Likely		**4**		Major		
5		Almost certain		**5**		Catastrophic		

14. Document history

Date	Substantive changes	Version
25/04/2025	• Full revision • NHS login added • Update to AI and automated decision-making	6.0
16/10/2025	• Integration with NHS App added	6.1
26/11/2025	• Updated document circulation information, logo and certification information.	6.2

15. Approval

Approval			
Name of Person(s) completing this document	Catherine McCrohan – Head of Operations @ Rapid Health	Date	16/10/2025
Data Protection Officer Review of document	Simon Santos – DPO/IGC @ 8fold Governance Ltd	Date	26/11/2025
SIRO Approval	Carmelo Insalaco – CEO @ Rapid Health	Date	26/11/2025

Appendix A – Template input to practice privacy policy wording

- The information below is to help practices update their privacy policy for Rapid Health.
- Practices **must** personalise it to match local policy and their usage of Rapid Health.
- Text in italics and/or square brackets identifies areas most likely to vary by practice but please check it all. “you” addresses the patient; “we”, “us” and “our” references the practice.

Using Rapid Health for online services

When you send a Rapid Health online request to us, you can do this from our website [or from the NHS App].

Looking after your information

We need to make sure you’re a registered patient at the practice and want to make sure you know about any request we get for you.

NHS login *[if your practice allows NHS login for Rapid Health]*

If you access Rapid Health using your NHS login details, the identity verification services are managed by NHS England.

NHS England is the controller for any personal information you provided to NHS England to get an NHS login account and verify your identity and uses that personal information solely for that single purpose. For this personal information, our role is a “data processor” only and we must act under the instructions provided by NHS England (as the “data controller”) when verifying your identity.

For more information on NHS login, see the NHS login privacy notice and NHS login terms and conditions.

NHS App *[if your practice allows NHS App for Rapid Health]*

You can access Rapid Health on the NHS App using your NHS login details.

If you sign in using NHS login, we will ask your permission to share your NHS login information with our service. This allows us to fill in some personal details for you, such as your name, date of birth and contact details.

We will not use your NHS login information for any other purposes. You can only share your NHS login information if you have proved your identity to NHS login.

You can choose not to share your NHS login information with Rapid Health but you will need to enter your information yourself whilst using the service.

For more information, see the NHS login privacy notice and NHS login terms and conditions.

[*Other*] information you provide to Rapid Health

GP practices are the data controller and Rapid Health is a data processor for information sent by patients to the practice using Rapid Health.

As data controller, the practice is responsible for keeping your information safe and explaining how it uses your information. There is a **How your information is used** box on the Rapid Health page where you give your name for a request, and further detail below.

[If you don't have an email address on your record

We allow patients without an email address on their record to send requests using Rapid Health but for your safety and security, these requests can't be offered appointment self-booking, as we need to check the patient identity first.]

Why we need an email address

We always email you to say we got your request. Something is wrong if you don't get a reply, so check your spam/junk folder if you don't see one. Send another request or call the practice if you don't get a reply within 15 minutes of sending your request.

We need to reply to you when we get a request. This reply says we got your request, what to expect and what to do if you are not well.

If you have an email address on your record, we can offer you self-booking, using the email address you put on your request (if a self-booking appointment is available).

Using a different email address

If you use a different email address for a request from the one on your patient record at your GP practice, we'll send replies to the email address you used for the request, but will also send a security email to the email address on your record.

Security emails say only that we got a request for you (or that an appointment was booked/changed/cancelled for you) and if this wasn't you, to contact the practice.

If a different email address is used for a request for a child from what is on their record, a security email is sent to the email address on their record.

Shared email addresses and devices

If you want to keep your requests private from someone you share an email address with, it's best to change your email address on your record. [*You can send us an **Update personal details** request. Our reply will just say we got a request from you – it will not say that you asked to change your details.]*

Our email replies

We send our reply and any appointment links to the email address you put on the request.

Our standard emails never repeat what you said in a request *[but if someone at your GP practice replies personally to your request, their reply may reflect information in your request]*. This reply will go to the email address you gave on your request.

The reply we send to the email address on a child's record (if there is one and it is different from an email address you use for a child request) just says we got a request for them and if this is a mistake to let us know – it does not say what kind of request.

Asking medical questions

If you want medical advice from the practice, we ask questions to check how soon you need this or if we need to suggest A&E to you. We ask this for your safety.

Why do you ask for Sex at Birth?

We ask this for your safety, so you can be asked the right medical questions.

Booking appointments online with us

There may be times when we send you a link to self-book an appointment with us, or you might book an appointment such as for a vaccination. Or you may want an appointment to discuss a medical concern.

Why do I need to provide information for these appointments?

When we send you a link to book into an appointment, we have 'pre-qualified' you for that appointment, so we only ask for some personal details before you book it.

Where you come to the website to book a type of appointment such as a vaccination or cervical smear test, we ask questions to check the appointment is right and safe for you.

If you want an appointment because you have a medical need, we ask questions to help us understand how soon to see you, or if we need to suggest A&E for your safety.

Keeping your personal data safe

How is my information stored?

Rapid Health stores the data on Amazon Web Services (AWS) servers in England. All data sent is encrypted when in transit (when it is sent) and at rest (when it is stored).

Patient data is managed as described in the NHS Records Management Code of Practice and stored on the practice system.

Rapid Health keeps a copy of requests for 400 days, for technical support purposes. They are deleted after the 400 days.

Can Rapid Health access the information?

Rapid Health must be able to access the information to meet its legal responsibilities as a data processor, for example to help the data controller (the practice) in providing subject access and allowing data subjects to exercise all their other rights under GDPR, and to provide technical support.

Only highly qualified technical staff with permission can access the data when the data controller asks for this, or if there is a technical problem. Strong controls are in place and a full audit trail kept.

Is Rapid Health NHS approved?

Yes. Rapid Health has passed all stages of assurance to interact with the practice patient record systems, EMIS and SystmOne.

What security credentials does Rapid Health have?

Rapid Health has completed NHS Data Security and Protection Toolkit assurance (under NHS ODS code 8KG49), and Cyber Essentials certification.

Rapid Health has successfully completed NHS Digital Technology Access Criteria assurance (under NHS ODS code 8KG49).

Rapid Health is fully compliant with DCB0129, which is for manufacturers of health IT software, and has a UKCA Class 1 medical device registered with the MHRA.

Rapid Health systems are independently penetration tested by an accredited CREST/CHECK supplier to CREST/CHECK standards at least once a year.

Is Rapid Health GDPR compliant?

Yes.

Note to practices:

Practices must include relevant sections only in their Privacy Policy so their patients can understand how their information is processed.

Practices should edit the information about Rapid Health services to make them accurate for their local usage of Rapid Health.

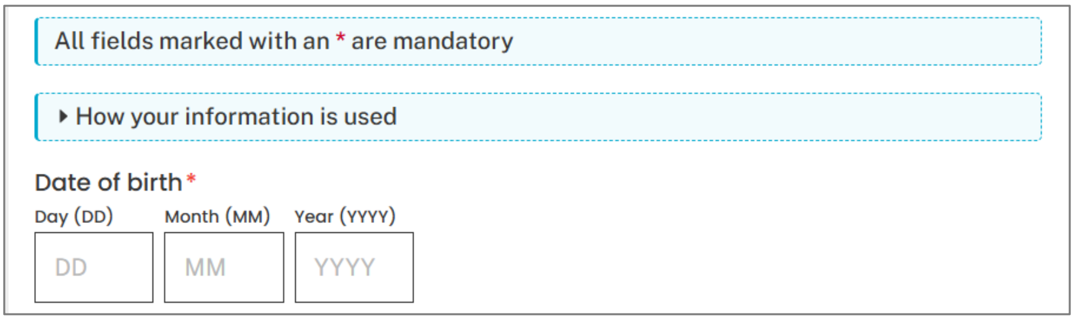
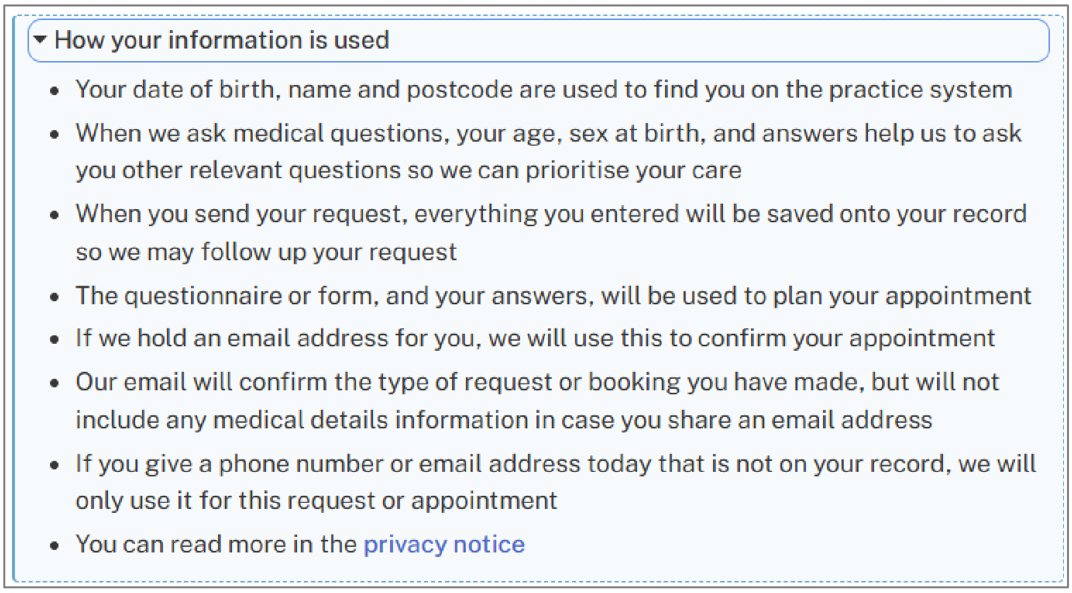
The NHS login [sic] and NHS App paragraphs are provided by NHS England and must not be changed. It must be removed if the practice has not enabled their patients to use it for Rapid Health.

Appendix B – Rapid Health privacy notice wording

Patient privacy notice

Rapid Health shows privacy information to the patient on the personal details page. A link to the Practice Privacy Notice is included there, so that the patient can read more on the practice website. Information on what the practice can include is provided in Appendix A.

The screenshots below show how the privacy notice is presented to patients providing their details.

When closed:	 All fields marked with an * are mandatory ▸ How your information is used Date of birth* Day (DD) Month (MM) Year (YYYY) DD MM YYYY
When open:	 ▾ How your information is used • Your date of birth, name and postcode are used to find you on the practice system • When we ask medical questions, your age, sex at birth, and answers help us to ask you other relevant questions so we can prioritise your care • When you send your request, everything you entered will be saved onto your record so we may follow up your request • The questionnaire or form, and your answers, will be used to plan your appointment • If we hold an email address for you, we will use this to confirm your appointment • Our email will confirm the type of request or booking you have made, but will not include any medical details information in case you share an email address • If you give a phone number or email address today that is not on your record, we will only use it for this request or appointment • You can read more in the privacy notice

Practice staff privacy notice

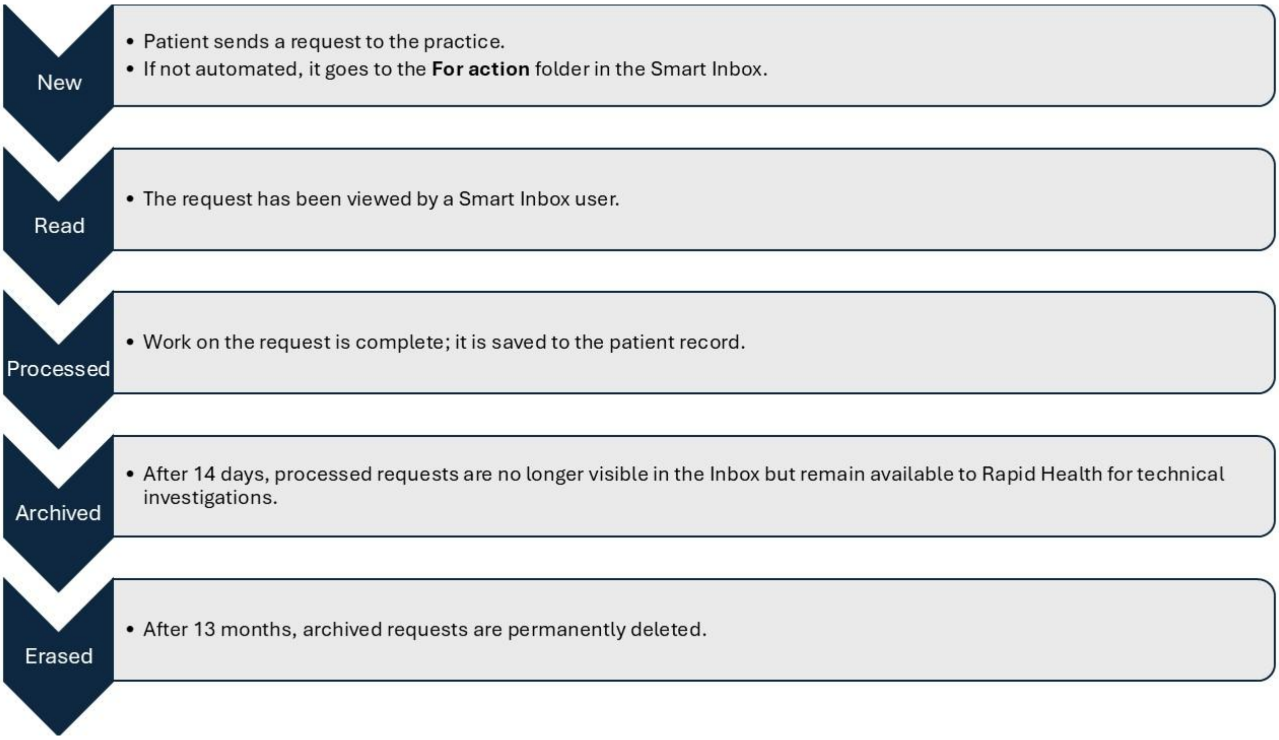
The Smart Inbox does not contain a privacy notice. As the employer and data controller, it is the responsibility of practices to ensure that practice staff understand that their professional personal data and activities are processed and retained in line with the Health and Social Care Act.

See the Data Collection Matrix in Appendix D for further information.

Appendix C – Data retention

Requests that go to the Smart Inbox for action should be processed in a timely way by the Practice.

The diagram below sets out the data retention lifecycle for patient requests and associated information. The first column is a system status (eg New, Processed) associated with each request.



New
- Patient sends a request to the practice.
- If not automated, it goes to the **For action** folder in the Smart Inbox.

Read
- The request has been viewed by a Smart Inbox user.

Processed
- Work on the request is complete; it is saved to the patient record.

Archived
- After 14 days, processed requests are no longer visible in the Inbox but remain available to Rapid Health for technical investigations.

Erased
- After 13 months, archived requests are permanently deleted.

Once processed, requests are archived after 14 days, then deleted after 13 months.

Practice activity history:
This information is retained with the patient requests for the same duration to support investigation and incident analysis.

Retention period rationale

GDPR requires that personal data should not be held unnecessarily. The requests that Rapid Health supports are transient and do not comprise clinical data. They are held to support what Practices may reasonably need in a short window after the request is sent to them, and subsequently for any need for incident investigation. The retention period is reviewed annually.

Patient records must be current, so Rapid Health data should be saved to the patient record promptly to ensure that it is available to anyone viewing the patient record. Two weeks' availability in the Smart Inbox is judged adequate.

The period of 400 days is designed to allow for evidence gathering in the event a patient takes action against a practice. This evidence would include the practice activity history (see above). Patients have a year to take action so 400 days allows time for the GP practice to notify Rapid Health.

This policy remains subject to review so that a balance is struck between holding the data 'just in case' and holding data for too long.

Appendix D – Rapid Health data collection matrix

User mission	User Action	Identifiable data	Data outcome	Other person to call (if proxy)	Non-identifiable data
Smart Inbox login **Data subject: practice staff**	Login	Email address / Username Password Authenticated session cookie (after login) IP address Device identifier	Request stored	Not applicable	n/a
Accept appointment invitation (Personal Direct Booking or Ask to Self-Book) **Data subject: patient**	Book appointment	First^ and last name DOB Address Phone number(s) Email address Practice system identifier NHS number Appointment slot identifier~	Request stored	Not applicable	Session cookie Consultation data
Seek admin support **Data subject: patient**	Submit request	First^ and last name DOB Address Phone number(s) Email Address Practice system identifier NHS number Administrative request parameters	Request stored	First and last name Phone number Relation	Session cookie
	Abandon during entry	None stored	No personal data stored	Not applicable	Session cookie

^ Middle names are not requested but are processed if provided.

~ Slot details may identify one or more specific members of practice staff

User mission	User Action	Identifiable data	Data outcome	Other person to call (if proxy)	Non-identifiable data
Seek medical advice **Data subject: patient**	Submit request and book appointment	First^ and last name DOB Address Phone number(s) Email address Practice system identifier NHS number Appointment slot Identifier~	Request stored	Not applicable	Session cookie Consultation data
	Submit request, no appointment offered	First^ and last name DOB Address Phone number(s) Email address Practice system identifier NHS number	Request stored	Not applicable	Session cookie Consultation data
	Abandon when no suitable appointments	First^ and last name DOB Address Phone number(s) Email address Practice system identifier NHS number	No personal data stored	Not applicable	Session cookie Consultation data
	Abandon when can't find condition	None stored	No personal data stored	Not applicable	Session cookie
	Abandon during questionnaire	None stored	No personal data stored	Not applicable	Session cookie
	Abandon during entry	None stored	No personal data stored	No data stored	Session cookie

^ Middle names are not requested but are processed if provided.

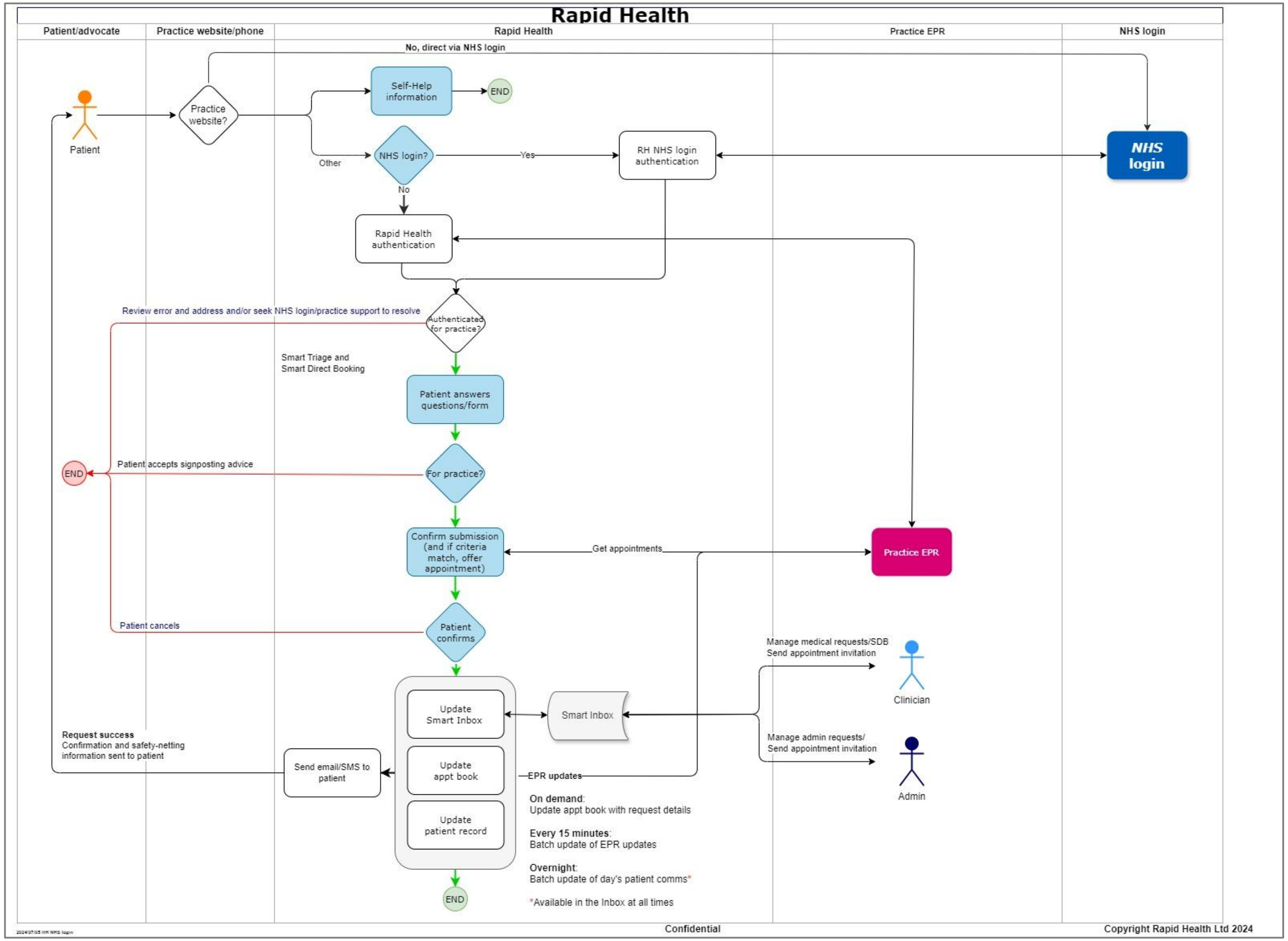
~ Slot details may identify one or more specific members of practice staff

User mission	User Action	Identifiable data	Data outcome	Other person to call (if proxy)	Non-identifiable data
Smart Direct Booking Data subject: patient	Submit request and book appointment	First^ and last name DOB Address Phone number(s) Email address Practice system identifier NHS number Appointment slot identifier~	Request stored	Not applicable	Session cookie Consultation data
	Submit request, no appointment offered	First^ and last name DOB Address Phone number(s) Email address Practice system identifier NHS Number	Request stored	Not applicable	Session cookie Consultation data
	Abandon when no suitable appointments	First^ and last name DOB Address Phone number(s) Email address Practice system identifier NHS number	No personal data stored	Not applicable	Session cookie Consultation data
	Abandon when can't find condition	None stored	No personal data stored	Not applicable	Session cookie
	Abandon during questionnaire	None stored	No personal data stored	Not applicable	Session cookie

^ Middle names are not requested but are processed if provided.
~ Slot details may identify one or more specific members of practice staff

Appendix E – Data flow map

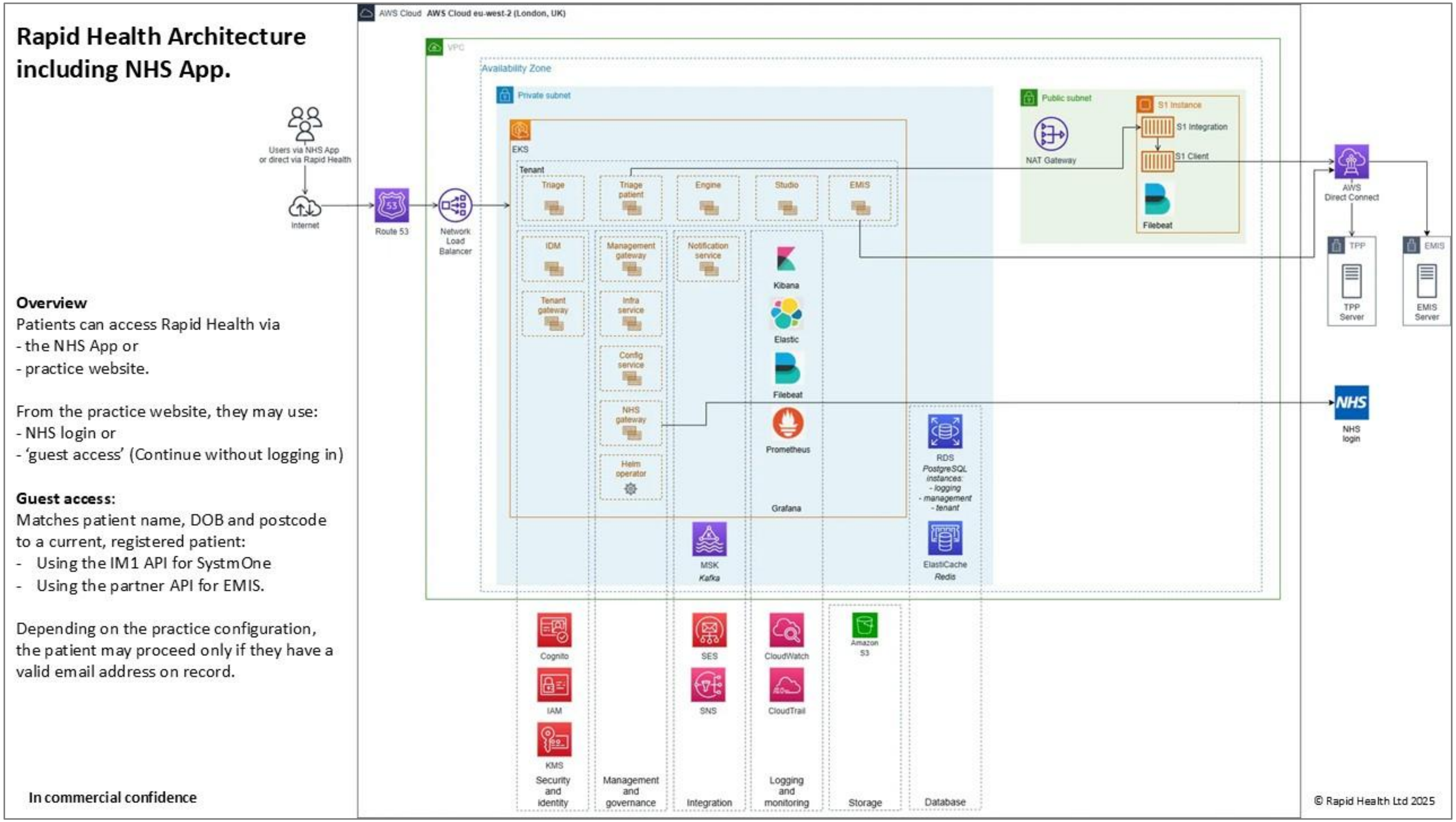
**** CONFIDENTIAL ****


Rapid Health
Patient/advocate
Practice website/phone
Rapid Health
Practice EPR
NHS login
No, direct via NHS login
Patient
Practice website?
Self-Help information
END
Other
NHS login?
Yes
RH NHS login authentication
NHS login
No
Rapid Health authentication
Review error and address and/or seek NHS login/practice support to resolve
Authenticated for practice?
Smart Triage and Smart Direct Booking
Patient answers questions/form
Patient accepts signposting advice
END
For practice?
Confirm submission (and if criteria match, offer appointment)
Get appointments
Practice EPR
Patient cancels
Patient confirms
Manage medical requests/SDB
Send appointment invitation
Clinician
Update Smart Inbox
Smart Inbox
Request success
Confirmation and safety-netting information sent to patient
Send email/SMS to patient
Update appt book
EPR updates
Manage admin requests/
Send appointment invitation
Admin
Update patient record
On demand:
Update appt book with request details
Every 15 minutes:
Batch update of EPR updates
Overnight:
Batch update of day's patient comms*
*Available in the Inbox at all times
END
2024/07/05 RH NHS login
Confidential
Copyright Rapid Health Ltd 2024

Appendix F – Logical architecture

**** CONFIDENTIAL ****

Rapid Health uses Amazon Web Services hosted on eu-west-2 (London, UK) to host its data. Each practice is given a separate tenant.



Rapid Health Architecture including NHS App.

Overview

Patients can access Rapid Health via
- the NHS App or
- practice website.

From the practice website, they may use:
- NHS login or
- 'guest access' (Continue without logging in)

Guest access:

Matches patient name, DOB and postcode to a current, registered patient:
- Using the IM1 API for SystmOne
- Using the partner API for EMIS.

Depending on the practice configuration, the patient may proceed only if they have a valid email address on record.

In commercial confidence