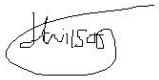
Data Protection Impact Assessment for GP Practice Use

DPIA Title:	accuRx Covid-19 Vaccine Booking Solution (accuBook)

Data Protection Officer consulted (date):	19th May 2021
Data Protection Officer comments:	None
Data Protection Officer signature:	
Caldicott Guardian consulted (date):	14th April 2025
Caldicott Guardian comments:	None
Caldicott Guardian signature:	
SIRO approval (date):	14th April 2025
SIRO comments:	None
SIRO signature:	

What is the process under consideration?	Guidance
The accuRx platform for Covid-19 vaccination appointment management feature (**accuBook**), is an IT product that has been developed to help healthcare providers of the vaccination service communicate with patients and coordinate bookings for their vaccinations. The aim of the accuBook solution is to enable for efficient communications between healthcare staff and patients to improve outcomes and productivity. AccuBook is a **web-based solution** which allows healthcare staff to: • create and manage vaccination clinics • invite patients to book themselves into these clinics, via SMS invites • book patients into clinics manually • manage which patients have booked, are yet to book, have declined to book, or have cancelled their booking • manage clinics on the day, recording which patients have arrived • access to pertinent patient information for a clinician to determine the safety of administering the vaccine. This process/function is only available if the accuTrack feature is in use by the end user and has been purchased by the vaccinating provider. AccuBook can be used to share and process personal and special category data about patients that is controlled by a healthcare provider organisation with other providers, if the organisation enables this. Where a practice is facilitating their own clinics and obtaining vaccinations directly to the surgery, they can manage their own vaccination clinics and invite their own patients to book. For practices vaccinating as a Primary Care Network (PCN), a lead practice will be nominated who will be in charge of creating and managing clinic times and dates. The lead practice will invite other practices within their group to have access to the clinics they have created. Each invited practice within a group can then invite patients to these clinics and manage their bookings. Information about all recorded vaccination events and adverse reactions will be automatically sent to NHS Digital in line with the requirements of the national Covid-19 vaccination programme, in order to update the National Immunisation Management Service (NIMS). Both features will also use personal data received from NIMS which is managed by NHS Digital. This DPIA describes the use of personal information in the accuBook solution. It also describes risks mitigated by design in the software and the ways in which the practice and the PCN can mitigate privacy risks.	Present a brief outline of the processing/scheme/project – i.e. the name of the project, reason for sharing data, etc

Will the process necessitate the use/processing/collection/sharing of any personal or pseudonymised data?	
Yes – personal and special category data will be processed for the purposes of the accuBook solution.	Personal data - Any information relating to an identified living person ('data subject') by way of an identifier such as a name, address, date of birth, NHS Number. Pseudonymised data - Personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, ie local identifier which would then be reidentified if needed.
What are the responsibilities linked to the processing? (ie who is the data controller, any possible data processors and joint data controllers)	
Individual GP practices are Data Controllers for personal data relating to their patients. AccuRx is the data processor, as per accuRx's Data Processing Agreement. GP practices collaborating to deliver the COVID-19 vaccination programme Enhanced Service (ES) are grouped together in Primary Care Network (PCN) groupings. Each practice within the grouping is a Data Controller in relation to their own patients' data. Every practice that makes up the primary care network is required by NHS England's Enhanced Service Specification to sign a Collaboration Agreement that must have *'appropriate arrangements for Patient record sharing in line with data protection legislation'*. This Collaboration Agreement between practices, and the Data Processing Agreement between each practice and accuRx will together govern the data processing involved for accuBook. The use of accuRx (and therefore agreement to its Terms and Conditions and the Data Processing Agreement) is a prerequisite for enabling the vaccine solution. This means that the Data Processing Agreement is in place with every healthcare organisation with access to the data processed in accuBook for their PCN Grouping. The Data Controller's and Data Processor's responsibilities are in line with processing personal data under the UK	Definition: Data Controller - Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

GDPR and Data Protection Act 2018 and are stipulated within the Data Processing Agreement between accuRx and the healthcare organisation. **Data Controller:** The healthcare organisations who enable the vaccine solution from accuRx are Data Controllers. In enabling the vaccine solution, the Data Controllers must have assurances from accuRx that they comply with the above requirements and have a valid **Collaboration Agreement** and **Data Processing Agreement** in place and comply with the Data Protection Act 2018 and all other relevant Data Protection legislation and standards. The Data Controller should therefore only upload patients who are eligible for the Covid-19 vaccination administered by their primary care network. The lead practice for the PCN grouping sets-up the designated site (where vaccinations are to be delivered) and allocates other healthcare organisations in their PCN grouping using their ODS codes. Each healthcare organisation (and therefore Data Controller) uploads the information about patients they wish to invite to vaccination at their PCN grouping site. **Data Processor:** AccuRx Ltd is the data processor for the accuBook solution. **Sub-processors:** The following sub-processors are used for the software platform for both accuBook: • Firetext Communications Ltd (UK based) - a third-party SMS gateway for the delivery of SMS messages. • BT Ltd (UK based) - a third-party SMS gateway for the delivery of SMS message. • Microsoft Azure Secure (UK based) - cloud hosting in accordance with NHS Digital guidance • NHSmail - process communications between healthcare and/or social care organisations • SendGrid ([UK GDPR Compliant] US) - accuRx use SendGrid for sending emails that don't contain patient identifiable information. It is used for forgotten passwords only. To provide support and communicate with its users, the accuRx uses: • TeamViewer UK Ltd (UK based) to gain remote access and support over the internet. • ActiveCampaign ([UK GDPR Compliant] US) as a CRM solution. • Intercom UK Ltd ([UK GDPR Compliant] US) a messaging application for providing online user support.	Definition: Data Processor - Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
What governance measures are in place to oversee the confidentiality, security, and appropriate use of the data?	

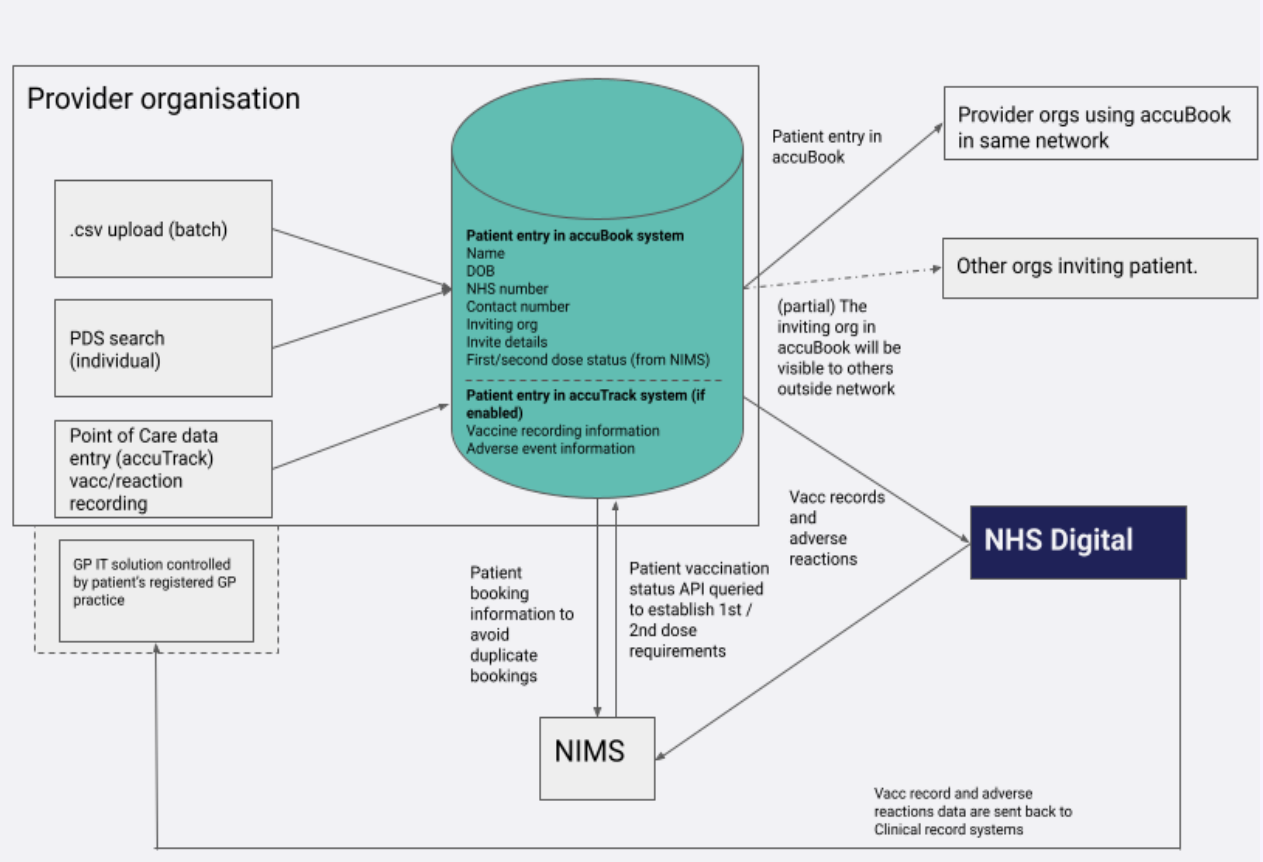
All computer equipment used in the GP Practice and by the lead healthcare organisation delivering the vaccine must comply with security requirements and adhere to the NHS standards for encryption. **Data Security and Protection Toolkit (DSPT) Compliance and Security Measures:** • GP practices submit a yearly DSPT submission and with MLCSU contracted by the CCGs to provide support to ensure practices can demonstrate their governance and data security compliance. Practices will be aiming for 'standards exceeded' in the 2020/21 submission due by June 30th 2021. • AccuRX has successfully completed the DSPT in 2019/20 and submitted to Standards Exceeded on 28/07/2020. They also hold both the Cyber Essentials and Cyber Essentials Plus certification. • The Data Processing Agreement outlines accuRx's responsibilities to ensure there are adequate technical and organisational controls in place to secure communications and protect patient confidentiality. • AccuRx's sub-processors are identified in its data processing agreement and operate based on Article 28 GDPR-compliant agreements. • AccuRx data is encrypted in transit via HTTPS and encrypted at rest via TDE. AccuRx follow the Microsoft Azure Security and Compliance Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. See here and here for further information. • The company's latest credentials can be found at https://www.accurx.com/security-and-privacy/our-resources. • API calls are used to send and retrieve data between accuBook and NIMS. API Security measures: The requests are made over HTTPS, using TLS v1.2 for transport security. AccuRx only send over the NHS number in the requests they make and no other personal information; NIMS require a valid time-limited token from accuRx and they do monitor activity sent using these tokens for any suspicious activity. **IG Training:** As part of the DSPT assertions, all staff within the above organisations must complete, as a mandatory requirement, annual data security awareness training. Each GP practice is required to provide its staff with appropriate information governance training to ensure compliance with data sharing arrangements, Common Law Duty of Confidentiality, UK GDPR, and the Data Protection Act 2018. All staff shall be made aware that any cases of inappropriate access and/or disclosure of patient information (whether inadvertently or intentionally) could face disciplinary action.	Governance measures may include compliance with the Data Security and Protection Toolkit, having IG, data security and data breach policies and procedures in place, 95% minimum staff compliance with IG training. Note that "All organisations that have access to NHS patient information must provide assurances that they are practising good information governance and use the Data Security and Protection Toolkit to evidence this by the publication of annual assessments" https://www.dsptoolkit.nhs.uk/Help/Attachment/5

DATA, PROCESSES AND SUPPORTING ASSETS

What is the data processed?	
The below is only limited to patients that practices choose to upload to the system - these are expected to be patients eligible to be offered the Covid-19 vaccine. **AccuBook Data:** ● **Patient data:** first and last name, NHS number, contact details [mobile], demographic data [DoB and gender], message content and vaccination appointment booking information (time/date and arrival status) and vaccination status (dates of flu and covid-19 vaccinations obtained from the National Immunisation Management Service) ● **System user data:** full name, identifiers, contact details (email), and activity data about their use of the accuRx platform. **Data retrieved from NIMS of those patients already uploaded into accuBook:** • Dates of patient's first and second Covid vaccinations • The specific product type of Covid vaccination product received (i.e. the product corresponding to 'Pfizer' or 'AstraZeneca' vaccine). • Flu vaccination date The following is an example of what an accuBook user can see for a patient who has been vaccinated once but has been sent an invite for their 2nd dose: *Vaccination details* ***Refresh NIMS Data*** *NIMS data last checked: Wednesday 7th April, 2021 at 12:19* *Vaccine type: Pfizer* *1st vaccination received: 24 Feb 2021*	List the data collected and processed, ie name, address, date of birth etc.

How does the life cycle of data and processes work?

The data flow diagram depicts the processing conducted in accuBook:

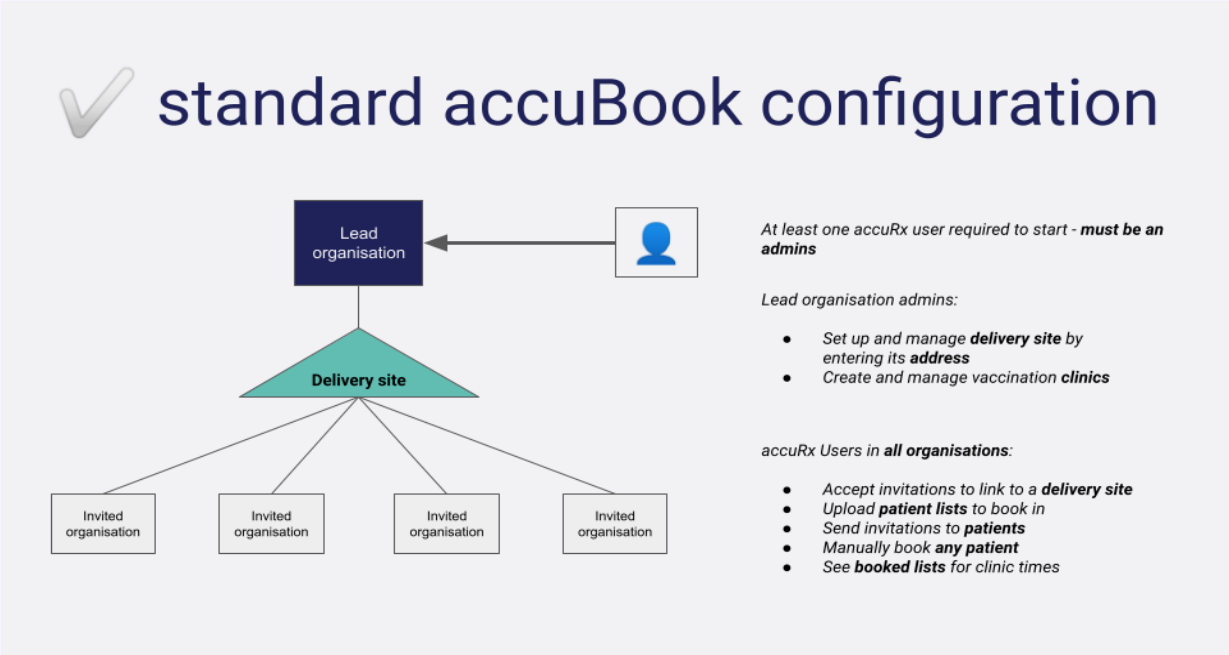


Present and describe how the product generally works (from the data collection to the data destruction, the different processing stages, storage, etc.), using for example a diagram of data flows (add it as an attachment) and a detailed description of the processes carried out.

The patient data can be provided by the practice providers into accuBook via three routes:

1. Organisations using accuBook **upload lists** of patients in the form of a .CSV spreadsheet. These lists can come from any source, but are usually extracted from the practice's own clinical system. Practice users can follow the accuRx's guide to ensure the process for upload is followed correctly. The guide to upload can be found here. The .CSV file contains:
    - Patient first and last name
    - Date of Birth (DOB)
    - NHS number
    - Contact phone number
2. An individual patient search can also be used to add a patient. Users of accuBook can perform **searches of the Personal Demographics Service (PDS)** using NHS number and DOB or a set of demographic information (name, DOB, gender, postcode). If an exact match is returned and the information available, that patient's details are copied into the list, with the same data items as listed above.
    - Some patients' entries on the PDS, or parts of them, are marked with a 'sensitive' flag. When search terms provided to the search function in accuBook and the API call made, no data is returned to accuRx about flagged records, or flagged parts of them.
    - The acceptable use of this feature is set out here. Practices should ensure that all users of accuBook and are aware of the parameters of this feature's use, which are within the overall purpose of managing and recording Covid-19 vaccinations.
3. Patients already uploaded into accuBook will have the following vaccination events retrieved from the **National Immunisation Management Service**:
    - Dates of patient's first and second Covid vaccinations
    - The specific product type of Covid vaccination product received (i.e. the product corresponding to 'Pfizer' or 'AstraZeneca' vaccine).
    - Flu vaccination date

The configuration diagram below shows how organisations are linked in a network to a lead organisation, which defines delivery site(s); approved users from other organisations can access the information uploaded to accuBook by a given practice:



Usage of data in accuBook:

Patient information is uploaded to a practice's accuBook system to manage the appointments of patients eligible for a vaccine. The patients are contacted via automated SMS invitations where they can self-serve and book directly themselves via the secure link provided via the SMS solution within accuBook or the practice can manually book patients into the accuBook system where patients are not able to self-serve. Appointments can be made at all clinics to which the inviting organisation is linked.

- Information of patients invited by practices can be viewed by accuRx users approved by admins in organisations linked to the same delivery site (see diagram above). This is so bookings can be managed and lists of booked patients can be viewed.
- The NHS numbers of patients who have a booking in accuBook are extracted nightly and shared with National Immunisation Management Service (NIMS). The NIMS service uses this information to ensure patients do not receive other invitations from the National Booking Service when they are

already booked in for an appointment through an organisation using accuBook, reducing the risk of duplicate bookings for the same dose. ● Vaccine recording and adverse reaction information is extracted nightly to NHS Digital to update the NIMS records for patients who had their vaccination record updated that day. ● Lead organisations in the accuBook network set up delivery site(s) and clinic times, associating the practices (via ODS code) with a delivery site. Practices then invite their own patients to book in, or trigger invitations to other patients. ● Practices can then view the patients invited in the same network. ● Admins at practices who are shown the invitation to join a network are told that accepting will mean information about patients they invite will be visible to approved users at other orgs in the network they join. **Patient invitations in accuBook:** Once the practices have uploaded the patient lists to accuBook, with valid contact information (mobile phone), this information can be reviewed/operated on by any user in an organisation linked to the 'inviting practice' by the invitation process. Patients with valid contact information can then be sent an SMS which is sent via and contained within the accuBook system. ● Patients receive an SMS with a unique link through which they can access a secure web form to book in their appointment in the clinics available at a delivery site. ● Patients enter their date of birth to verify they are the patient associated with the phone number in their record. ● Patients self-book their vaccination appointments. ● Patients receive reminders and automatic call/recall via SMS for the course of vaccinations. ● Practice users can manually book in patients who cannot receive SMS messages.	
What are the data supporting assets?	
• GP Practice System of Choice (for example EMIS/SystmOne) • Desktop computer or mobile device (laptop, tablet, smart phone) • accuRx, accuBook solution • Secure internet network • .csv spreadsheet (Microsoft Excel) • IT APIs	List the data supporting assets (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.)

Fundamental principles

PROPORTIONALITY AND NECESSITY

Are the processing purposes specified, explicit and legitimate?	
The processing of patient data for the use of accuBook is necessary and proportional for the purposes of running a vaccination programme. The purpose of the solution is to allow healthcare staff to communicate with patients (and each other regarding patients) for the provision of healthcare services and is specifically designed to support the Covid-19 vaccination programme. The personal data processed within accuBook are only available to organisations providing Covid-19 vaccines in line with the requirements of national programmes in England. The solution is NHS Digital-assured for appointment management. The system must only be used for the purposes of inviting patients to Covid-19 vaccination appointments, managing those appointments, and for the recording of those vaccinations and any adverse events. Any use outside of these purposes is in breach of the terms and conditions of accuRx's services and the Data Processing Agreement between the two organisations. The legal basis is specified for the provision of direct care and for the reasons of public interest, in the area of public health.	Explain why the processing purposes are specified, explicit and legitimate. How is the legal basis being specified?

What is the lawful basis for processing the data?	
The lawful basis for processing the data is the provision of direct patient care, which is defined under Articles 6 and 9 of the General Data Protection Regulations (GDPR) and aligned through the Data Protection Act 2018. Article 6 defines the legal basis with article 9 a requirement when using special categories of data. ***Article 6*** 6(1)(e) processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller. ***Article 9*** 9(2)(i) processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy". The relevant basis in UK law is set out in the DPA 2018, in Schedule 1 condition 3. In order to rely on this condition the processing must be carried out either: • by, or under the responsibility of, a health professional; or • by someone else who in the circumstances owes a legal duty of confidentiality. This condition can apply where the processing is necessary for: **public vaccination programmes.** 9(2)(h) processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, **medical diagnosis, the provision of health or social care or treatment or management of health or social care systems** and services on the basis of Union or Member State law or a contract with a health professional. Obligation of professional secrecy: for the purposes of Article 9(2) (h) of the GDPR, the circumstances in which the processing of special category personal data is carried out is subject to the "conditions and safeguards" referred to in Article 9(3) of the GDPR (obligation of professional secrecy). Therefore, in accordance with DPA Section 11(1), these "conditions and safeguards" include circumstances in which it is carried out – • by or under the responsibility of a health professional or a social work professional, or • by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.	What is the legal basis for processing the data? – direct care, legislation or consent, (don't forget, consent should be a last resort and only used if there is no direct care or legislation in place). Remember to identify which Article 6 or 9 conditions will be used and if there is supporting legislation, what that legislation is, including the specific section of the legislation which supports the use of data for this purpose.

Regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) to require health and care organisations to process confidential patient information in the manner set out below for purposes set out in Regulation 3(1) of COPI: (a) diagnosing communicable diseases and other risks to public health; (b) recognising trends in such diseases and risks; (c) controlling and preventing the spread of such diseases and risks; (d) monitoring and managing— (i) outbreaks of communicable disease; (ii) incidents of exposure to communicable disease; **(iii) the delivery, efficacy and safety of immunisation programmes;** (iv) adverse reactions to vaccines and medicines; (v) risks of infection acquired from food or the environment (including water supplies); (vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.	
Is the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?	
The processing is necessary and proportional for the purposes of running a vaccination programme. The booking solution processes no more additional data items than the wider accuRx platform, other than the data relating to a patient's booking text messages, and the slots they book themselves into. The data shared will be limited to what is necessary to provide the vaccination service to these patients safely. Only patients uploaded to the system can be shared with the users managing the delivery site.	Need confirmation in here that there is no personal data being processed that isn't absolutely necessary for the purpose of the project. Is any information being collected that isn't required to complete the project?
Is the data accurate and kept up to date?	
It is the GP practices' responsibility, in their role as Data Controller, to ensure the patient records are up to date and accurate prior to upload to the accuBook platform. Practices must therefore have data quality procedures in place and ensure all staff are trained on how and when to update records. Regular audits must also be completed to ensure the patient records remain accurate and up to date.	Describe what steps are taken to ensure the quality of the data. Need confirmation here of who will check the data is accurate and what process is in place to ensure the data is kept up to date.

What is the storage duration of the data?	
Patients' data is retained in line with the NHS Records Management Code of Practice 2020. However, accuRx will delete the data earlier than suggested by this code if they were informed by controller, subject, or other authority, that the condition of Article 9(3) GDPR and s. 11(1) Data Protection Act 2018 no longer applies. NHS Digital are expected to issue guidance on retention for all solutions commissioned on appointment management and recording solutions - this will inform the accuRx Vaccine Booking and Recording Solutions default retention period. Deletion will be carried out at the data controllers' request or when a service with the organisation in control of the data is terminated. AccuRx retains the data pertaining to users for as long as necessary for the purpose of providing the service (i.e. continuing to have an account with accuRx) or to complete a transaction (e.g. measuring use of the platform for billing purposes) or they are instructed to delete the user account. Data may be shared with sub-processors (see full list above under the responsibilities linked to the processing section) such as cloud services used for accuRx's own storage, communications, security, engineering, and similar purposes. AccuRx's sub-processors operate based on Article 28 GDPR-compliant agreements and are listed within the Data Processing Agreement between practices and accuRx.	Ideally there will be a list here of all the data assets being processed, how long they will be held for, where the timescales have come from (i.e, Information Governance Alliance code of practice for records management). This should be stated for each organisation that holds the data. Records Management Code of Practice for Health and Social Care 2016: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

How are the data subjects informed of the processing?	
To support transparency of the data processing being carried out by accuRx on behalf of practices, each practice will need to inform their patients of the use of the accuRx solution through inserting a description of the practice's use of the accuRx platform via their practice privacy notice for patients. They should add explicit reference to the vaccine booking solution (accuBook) and any required onward data sharing to NHS Digital or the NIMS and the reason why that information can be passed there. This applies to individual-level data	In here you would expect that privacy notices are made available to the data subjects and information and advice, perhaps even leaflets, about how data subjects can access privacy notices.

that is to be passed to NHS Digital to monitor the completion of vaccination appointments in the booking solution. **Consultation process:** The Covid-19 vaccination programme has been planned quickly. The specification for the primary care Enhanced Service was published on the 1st December 2020. Therefore, limited time for consultation on this product has been available. Nonetheless, accuRx has engaged widely with practices, PCNs, NHS Digital and NHS England, and patients to understand their needs and expectations from software solutions that will support the vaccination programme. The solution is designed adhering to national specifications from NHS Digital. It is also built-in close alignment to the Enhanced Service specification, and with flexibility given that the requirements on practices might change. It is the responsibility of every GP Practice to ensure that as Data Controllers, they inform their patients under the 'Right to be Informed' detailed in the Data Protection Act 2018. They must ensure the use of accuRX is detailed in their practice privacy notice and uploaded both to the website and within practice. Any easy-to-read privacy notices, notices produced in other formats or notices translated into other languages, must also contain this information. Practices may wish to produce information leaflets on the use of accuRX or signpost patients to the accuRX website for additional information, but the information cascaded to patients must be transparent, easy to understand and specific. AccuRX have a data security and privacy notice on their website and provide a page designated for patients to explain its role in communication and patient data use. The following link can be referred to within the practice privacy notice for patients. https://www.accurx.com/security-and-privacy/for-patients	
If consent is your lawful basis how is the consent of data subjects obtained?	
Consent is not the lawful basis. Any patient who does not wish to be contacted for a vaccination booking via accuRx would simply not access the link provided and make their preferences to the GP Practice.	If consent is not your legal basis, then this should say not applicable. If consent is the legal basis, then this should advise how the consent is obtained, what information is given to the data subject when obtaining consent about what data will be used and for what purpose, how the consent is recorded and what information is given to the data subject about how they can withdraw their consent.

How can data subjects exercise their rights of access and to data portability?	
The GP Practice will process any subject access requests made by patients adhering to the practice Subject Access Request policies. Any information updated into the records following an accuRX consultation will form part of the release of records and will also adhere to the stipulations of the accuRX data processing agreement. Patients have the right to request their information in any accessible format in relation to their right to their right of access. The right to data portability does not apply to the legal bases used for the processing of personal and special category data for the accuBook solution. The right to data portability only applies when lawful basis for processing is under consent **or** for the performance of a contract; and processing by automated means.	Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests
How can data subjects exercise their rights to rectification and erasure?	
Under Article 16 of the GDPR data subjects have the right to have inaccurate data rectified. The GP Practice in their role as data controller must ensure that they have robust policies in place to ensure patients can request rectification of their information and forms part of the Data Quality process each practice must implement to ensure records are accurate and kept up to date. In relation to erasure, this must only be done in cases where clinical validation has been received and where personal data is inaccurate. In addition, practices have a legal requirement under The Public Records Act 1958 to maintain medical records and, as such, cannot erase factually accurate clinical information upon request. In line with the ICO guidelines, requests for erasure must obtain prior clinical validation and only be considered on a case-by-case basis.	Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests
How can data subjects exercise their rights to restriction and to object?	
A data subject can exercise their right to restrict and to object when the legal basis relies on public task, carrying out the data processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. It is harder to restrict or object when the purpose meets direct care purposes however the data subject must give specific reasons why they object to the processing of their data and the reasons need to be based on their particular situation. The GP practice must clearly detail the rights and freedoms of the individual in the practice privacy notice.	Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests

If there is a Data Processor involved, are the obligations of the processors clearly identified and governed by a contract?	
Data processor obligations are defined within the following contract between the GP practice and accuRx: Data Processing Agreement The use of accuRx (and therefore agreement to its Terms and Conditions and the Data Processing Agreement) is a prerequisite for enabling the vaccine solution. This means that the Data Processing Agreement is in place with every healthcare organisation with access to the data processed in accuBook for their PCN Grouping. The Data Controller's and Data Processor's responsibilities are in line with processing personal data under the UK GDPR and Data Protection Act 2018 and are stipulated within the Data Processing Agreement between accuRx and the healthcare organisation.	If a data processor is involved, this should fully explain who the processor is and what their role is in relation to the processing. Need confirmation that there is a data processing agreement and/or contract in place between the data controller and the data processor which stipulates what the data processor will be doing with the data. If there is no data processor, then consideration should be made to a data sharing agreement being put in place.
In the case of data transfer outside the United Kingdom, are the data adequately protected?	
For the accuBook solution no personal or special category data will be transferred or stored outside the UK.	This should confirm if any data is being transferred outside of the UK, this includes where servers, for systems being used, are based. If data is being transferred outside of the UK, then strict assurances need to be in place that where the data is being transferred to will meet GDPR compliance and a contract in place.

Risks

This section allows you to assess the privacy risks, taking into account existing or planned controls.

Risk Factors to consider:

- Illegitimate access to data;
- Unwanted modification of data
- Data disappearance

PLANNED OR EXISTING MEASURES

See appendix A for information on working out Risk Likelihood and Severity

#	Risk Ref	Risk Description	Mitigating Control(s)/Actions	Likely	Severity	Score
			(See details below)	**(See details below)**		
1	Governance	Access to Personal data by persons other than the data subject or legitimate user of the solution	Healthcare professionals are authenticated by requiring: NHSmail to register for an account; TPP SystmOne or EMIS Web profiles; and an administrator at their GP practice to approve them. This is to prevent people who do not actually and currently work at the provider organisation from accessing the accuRx system. Patient demographic data is only pulled from either TPP SystmOne or EMIS Web principal care systems. This ensures that a healthcare professional can only access data of patients	Low	Significant	Low

			registered at their practice or those covered by the Collaboration Agreement. Mobile devices with web access controlled on-site. Standard security features and procedures (e.g. auto-locking and passcodes) of these devices will be used to limit access to their contents by non-staff.			
2	Malware	The integrity of the computers used (how at risk are they from trojans or viruses)	Likely that the point of care solution run on mobile devices, with greater degree of protection against malware. Desktop computers may also be used since this is a web platform, but these devices are subject to same high NHS data security standards for GP practices and other NHS providers - such as the Data Security and Protection Toolkit.	Low	Minor	Low
3	GDPR	Patients impersonating eligible patients in order to receive the Covid-19 vaccine	Low underlying likelihood as they'd have to already impersonate to persuade practice to change contact information. Practices are currently subject of a national campaign to ensure patient contact information is up to date for this vaccine programme. Patients can contact practice themselves if a malicious actor somehow obtained access to their unique invitation link. Healthcare professionals will appropriately verify identity on-site at point of care in line with usual practice and vaccine service specification. Any proven victim of impersonation can have their record corrected, and vaccine administered.	Low	Low	Low
4	GDPR	There is a risk that PDS information being reliant upon information supplied by the GP so there is a risk of incorrect patient details.	GP practices adopt and implement effective data quality protocols, regular record keeping and data protection audits and reviews. As a matter	Medium	Significant	Low

			of good practice and in line with record keeping standards, practices will regularly check patient demographic details for accuracy and any updates. The NHS number is used as the primary identifier to minimise the risk of clinical entries and data being included within the wrong patient record.			

EXAMPLES of risks - FOR INFORMATION ONLY	
Education	Breach of IG policies and guidance due to lack of visibility, communication and training
GDPR	Non-compliant with GDPR implementation
Malware	Threat from malicious links/ attachments
Process	Information is lost/ processed in a non-compliant manner due to gaps in processes and poor controls
Purchasing	Limited governance over low spends allows DPIA process bypass
Sharing	Sharing information inappropriately or illegally due to immature technology or understanding of legislation
Supplier	Suppliers breach Privacy Law due to poor information handling practices/ IT security

Appendix A

Encryption	Means implemented for ensuring the confidentiality of data stored (in the database, in flat files, backups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.). Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the processing.
Anonymisation	Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose. Remember to clearly distinguish between anonymous and pseudonymous data.
Partitioning	Implementation of data partitioning helps to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur.
Logical Access Control	Methods to define and attribute users' profiles. Specify the authentication means implemented. Where applicable, specify the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.).
Traceability (logging)	Policies that define traceability and log management.
Archiving	Where applicable, describe here the processes of archive management (delivery, storage, consultation, etc.) under your responsibility. Specify the archiving roles (offices of origin, transferring agencies, etc.) and the archiving policy. State if data may fall within the scope of public archives.
Paper document security	Where paper documents containing data are used during the processing, indicate here how they are printed, stored, destroyed and exchanged.

Minimising the amount of personal data	The following methods could be used: Filtering and removal, reducing sensitivity via conversion, Reducing the identifying nature of data, Reducing data accumulation, Restricting data access

Physical Security Control

Operating security	Policies implemented to reduce the possibility and the impact of risks on assets supporting personal data.
Clamping down on malicious software	Controls implemented on workstations and servers to protect them from malicious software while accessing less secure networks.
Managing workstations	Controls implemented on workstations (automatic locking, regular updates, configuration, physical security, etc.) to reduce the possibility to exploit software properties (operating systems, business applications etc.) to adversely affect personal data.
Website security	Implementation of ANSSI's Recommendations for securing websites.
Backups	Policies and means implemented to ensure the availability and/or integrity of the personal data, while maintaining their confidentiality.
Maintenance	Policies describing how physical maintenance of hardware is managed, stating whether this is contracted out. Indicate whether the remote maintenance of apps is authorized, and according to what arrangements. Specify whether defective equipment is managed in a specific manner.

Processing Contracts	Regulate the procurement relations via a contract signed intuitu personæ. - Require the processor to forward its Information Systems Security Policy (PSSI) along with all supporting documents of its information security certifications and append said documents to the contract. Ensure that the measures pursuant to its PSSI comply with the ICO's recommendations in this respect. - Precisely determine and set, on a contractual basis, the operations that the processor will be required to carry out on personal data: 1) The data to which it will have access or which will be transmitted to it. 2) The operations it must carry out on the data. 3) The duration for which it may store the data. 4) Any recipients to which the data controller requires it to transmit the data. 5) The operations to be carried out at the end of the service (permanent deletion of data or return of the data in the context of reversibility then destruction of data at the processor's). 6) The security objectives set by the data controller. - Determine, on a contractual basis, the division of responsibility regarding the legal processes aimed at allowing the data subjects to exercise their rights. - Explicitly prohibit or regulate use of tier-2 processors. - Clarify in the contract that compliance with the data protection obligations is a binding requirement of the contract.
Network security	Depending on the type of network on which the processing is carried out (isolated, private or Internet). Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.
Physical access control	Policies to ensure physical security (zoning, escorting of visitors, wearing of passes, locked doors and so on). Indicate whether there are warning procedures in place in the event of a break-in.

Monitoring network activity	Monitor intrusion detection systems and intrusion prevention systems in order to analyse network (wired networks, Wi-Fi, radio waves, fibre optics, etc.) traffic in real time and detect any suspicious activity suggestive of a cyber-attack scenario.
Hardware security	Indicate here the controls bearing on the physical security of servers and workstations (secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.).
Avoiding sources of risk	Documentation on implantation area, which should not be subject to environmental disasters (flood zone, proximity to chemical industries, earthquake or volcanic zone, etc.). Specify if dangerous products are stored in the same area.
Protecting against non-human sources of risks	Policies describing the means of fire prevention, detection and fighting. Where applicable, indicate the means of preventing water damage. Also specify the means of power supply monitoring and relief.

Organisational Control

Organisation	Specify whether a person is responsible for the enforcement of privacy laws and regulations. Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy.
Policy	Set out important aspects relating to data protection within a documentary base making up the data protection policy and in a form suited to each type of content (risks, key principles to be followed, target objectives, rules to be

	applied, etc.) and each communication target (users, IT department, policymakers, etc.).
Managing Privacy risks	Policy describing processes to control the risks that processing operations performed by the organization pose on data protection and the privacy of data subjects (building a map of the risks, etc.)
Integrating privacy protection in projects	Existence of a policy designed integrate the protection of personal data in all new processing operations.
Managing personal data violations	Existence of an operational organization that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.
Personnel management	Existence of a policy describing awareness-raising controls are carried out with regard to a new recruit and what controls are carried out when persons who have been accessing data leave their job.
Relations with third parties	Existence of a policy and processes reducing the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy.
Supervision	Existence of a policy and processes to obtain an organization able to manage and control the protection of personal data held within it.

Severity Definitions

Severity	Description
Negligible severity	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.

	Examples: - physical : transient headaches - material : loss of time in repeating formalities or waiting for them to be fulfilled, receipt of unsolicited mail (e.g.: spams), reuse of data published on websites for the purpose of targeted advertising , etc., - moral : mere annoyance, feeling of invasion of privacy without real or objective harm (commercial intrusion), etc.
Limited severity	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties Examples : - physical : minor physical ailments (minor illness due to disregard of contraindications), defamation resulting in physical or psychological retaliation, etc. - material : Unanticipated payments (fines imposed erroneously), denial of access to administrative or commercial services , Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects, etc. - moral : minor but objective psychological ailments, feeling of invasion of privacy without irreversible damage, intimidation on social networks, etc.
Significant severity	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties Examples: - physical : serious physical ailments causing long-term harm (worsening of health due to improper care, or disregard of contraindications), lteration of physical integrity for example following an assault, an accident at home, work, etc. - material : misappropriation of money not compensated, targeted, unique and non-recurring, lost opportunities (home loan, refusal of studies, internships or employment, examination ban), loss of housing, loss of employment, etc. - moral : serious psychological ailments (depression, development of a phobia), feeling of invasion of privacy with irreversible damage, victim of blackmailing, cyberbullying and harassment, etc.

Maximum severity	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome Examples : - physical : long-term or permanent physical ailments, permanent impairment of physical integrity, death - material : financial risk, substantial debts, inability to work, inability to relocate, loss of evidence in the context of litigation, loss of access to vital infrastructure (water, electricity), etc. - moral : long-term or permanent psychological ailments, criminal penalty, abduction, loss of family ties, inability to sue, change of administrative status and/or loss of legal autonomy (guardianship), etc.

Severity	Description
Negligible likelihood	It does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader and access code).
Limited likelihood	It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader).
Significant likelihood	It seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in offices that cannot be accessed without first checking in at the reception).

Maximum likelihood	It seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in the public lobby).

Risk Mapping

In accordance with the **Risk Treatment Process**	
Score	Risk Class
1	Negligible
2	Limited
3	Significant
4	Maximum

		Severity			
		Negligible (1)	**Limited (2)**	**Significant (3)**	**Maximum (4)**
Likelihood	**Maximum (4)**	Medium (4)	High (8)	Very High (12)	Very High (16)
	Significant (3)	Medium (3)	High (6)	High (9)	Very High (12)
	Limited (2)	Low (2)	Medium (4)	High (6)	High (8)
	Negligible (1)	Low (1)	Low (2)	Medium (3)	Medium (4)