****

**accuRx DPIA Template: Covid-19 Vaccine booking and recording**

This template closely follows the ICO’s example of how you can record your DPIA process and outcome. It follows the process set out in the ICO’s DPIA guidance, and should be read alongside that guidance and the [criteria for an acceptable DPIA](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711) set out in European guidelines on DPIAs.

**NB: As the data controller, when using accuRx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template to describe how our software service processes personal data.**

Submitting Controller Details

|  |  |
| --- | --- |
| Name of controller | The Strand Medical |
| Subject/title of DPO | AccuRX Covid 19 vaccine Booking and recording |
| Name of controller contact / DPO | Trudy Slade |

Step 1: Identify the need for a DPIA

|  |
| --- |
| Summarise why you identified the need for a DPIA. |
| accuRx’s mission is to improve communications between healthcare staff and patients.  Using the vaccine appointment management feature (accuBook) in the accuRx platform will help the providers of the vaccination service communicate with patients and coordinate bookings for their vaccinations.  Using the vaccine recording feature (AKA accuTrack - TBC) will enable staff working at the vaccination centre to capture information about the vaccination event, and any adverse reactions.  Both features can be used to share personal information about patients that is controlled by a provider organisation with other providers if the organisation enables this.  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 is managed by NHS Digital.  The use of both features can involve processing special category personal data about patients.  This DPIA describes the use of personal information in the software platform, and the data sharing arrangements. It also describes risks mitigated by design in the software. It also describes the ways in which The Strand Medical can mitigate privacy risks. |

|  |
| --- |
| Step 2: Describe the processing |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? |
| To support transparency of the data processing being carried out by accuRx on behalf of the organisation completing this DPIA, the organisation may choose to inform patients of the use of the accuRx solution through inserting a short summary into their privacy notices.  accuRx provides a [page designed for patients](https://www.accurx.com/security-and-privacy/for-patients) to explain its role in communication and patient data use that you are welcome to refer to.  Specific guidance on how to set out your privacy notice is widely available. For example, the BMA provides [for GP practices here](https://www.bma.org.uk/advice-and-support/ethics/confidentiality-and-health-records/gdpr-privacy-notices-for-gp-practices).  accuBook and accuTrack are designed to support the Covid-19 vaccination programme. They are only available to organisations providing Covid-19 vaccines in line with the requirements of national programmes in England. Both are NHS Digital assured solutions for Appointment Management and Vaccine Recording respectively.  They 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 data flow diagram here depicts the processing conducted in accuBook:  [**Data flows for accuRx vaccine booking and record solutions**](https://docs.google.com/presentation/d/1UNZAuK8e6TXiLOJLPGC0Kvec37MFYewWdxCNHyzrmIk/edit?usp=sharing)  The configuration diagram here 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 and accuTrack**  Patient information uploaded to a practice’s accuBook system is used to manage the appointments of patients, through automated SMS invitations with self-serve booking links or manual bookings. 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. This is so bookings can be managed and lists of booked patients 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**  Patients uploaded with valid contact information (mobile phone numbers) can then be sent an SMS.   * 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 can not receive this message.   **accuTrack Recording solution**  Approved users can view a treatment screen for each patient booked in for a clinic in the networks they are part of. The data a user can view about patients is limited to what is necessary to administer the vaccine safely. They can currently view data about patients shared from other organisations working in the accuBook network. Like any way to create records of patient information, users should be trained to only access this page when necessary. That should only be when they are required to make this recording on behalf of a vaccinator.   * Patients are listed against their booked appointment slots, with name, NHS number, DOB and gender. * Patients can be marked as arrived and a ‘treatment screen’ can be navigated to. * Treatment screen displays the vaccination history information of a patient retrieved from NIMS. * Treatment screen is used for data capture by accuRx users. For each patient, a structured treatment record is created in line with NHS Digital Covid-19 vaccine solution spec for the vaccination data extract. This includes:   + Covid-19 vaccine received, along with batch number   + Which dose in course of treatment   + Status of patient consent to the vaccination   + Injection site   + Vaccinating member of staff   + Results of treatment screening questions   + Notes made in free-text by staff member.   + Individual adverse reactions. * The vaccination record will be saved back to the individual patient’s record in their GP practice’s clinical IT system (EMIS/TPP) in a standardised form. * Practices are expected to provide daily data extracts on vaccination events recorded in an approved delivery site. These are due to be provided nightly to NHS Digital, but will eventually become an hourly update. This will include personally identifiable data shared to the National Immunisation Management Service (NIMS), and also individual level data about vaccinated patients to ensure that the practice is paid for their successfully vaccinated patients. |

|  |
| --- |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| The data processed in accuBook all relates to the health or health care of an individual; it is therefore considered special category data.  **Data sources in accuBook and accuTrack**  Data is provided by the providers into accuBook in three routes:   * Organisations using accuBook and accuTrack **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. They contain:   + First and last name   + Date of Birth (DOB)   + NHS number   + Contact phone number * 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 person’s details are copied into the list, with the same data items as above.   + Some patients’ entries on the PDS, or parts of them, are [marked with a ‘sensitive’ flag](https://digital.nhs.uk/services/national-back-office-for-the-personal-demographics-service/management-of-nhs-numbers-and-pds-records). 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](https://drive.google.com/file/d/1jO2zxBkzkWv0K4A4KP9uZ3YZHDRUfTSZ/view?usp=sharing) of this feature is set out here. [The organisation completing this DPIA should ensure that all users of accuBook and accuTrack are aware of the parameters of this feature’s use, which are within the overall purpose of managing and recording Covid-19 vaccinations]. * Patients already uploaded into accuBook will have the following vaccination events retrieved from the [**National Immunisation Management Service**](https://www.england.nhs.uk/contact-us/privacy-notice/national-flu-vaccination-programme/):   + 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 individual-level patient data processed in the booking solution is limited to:   * **Demographic and contact data** (typically name, identifiers, contact details [mobile], demographic data [DoB; gender]) * **Message content** and **vaccination appointment booking information** (time/date, invite and booking status, booking notes, and arrival status) * **Vaccination status** (dates of flu and covid-19 vaccinations obtained from the National Immunisation Management Service)     **Recording solution:**  When the recording solution is enabled, the additional data processed by AccuRx in this case is:   * **Records of vaccinations and adverse events** (created in vaccine recording solution) * These will be extended in line with the vaccination programme’s requirements, as defined in the [NHS Digital specifications here](https://gpitbjss.atlassian.net/wiki/spaces/CVPDR/pages/7918551342/Vaccination+and+Adverse+Reaction+Recording). For example, we know this will include the ethnicity of the patient being vaccinated, as recorded at the point of care.   **Retention**  Patients’ data is generally retained in line with the [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). 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’s sub-processors are identified in its [data processing agreement](http://accurx.com/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 Compliant Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. See [here](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/health-and-social-care-cloud-security-good-practice-guide) and [here](https://docs.microsoft.com/en-gb/azure/storage/common/storage-service-encryption) for further information. |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| The nature of the relationship between practice and the individual patient is that of health and social care staff providing direct care to patients. These patients are those eligible and invited for the Covid-19 vaccination programme.  Use of the vaccine product depends on the practice already using the accuRx Desktop platform at the practice (DPIA template for accuRx desktop [here](https://docs.google.com/document/d/1BYsv5iadneb6fJih_uAr1J26lSv7x4X-zVfCGA0nTZ4/edit?usp=sharing)).  The Recording solution involves the creation of an individual record of Covid-19 vaccination that is to be shared by the organisation with the National Immunisation Management Service (NIMS) as a condition of their participation in the Covid-19 vaccination programme. The accuRx solution will format the data according to NHS Digital specifications (available on request). Once the data is passed to NIMS, it is no longer being processed by accuRx. The NIMS service is described by NHS England [here](https://www.england.nhs.uk/contact-us/privacy-notice/national-flu-vaccination-programme/). |

|  |
| --- |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
| accuRx always acts as a data processor in relation to patients’ data that providers share with accuRx through the use of its software services.  Health care providers’ lawful basis for processing patient data using accuRx services is expected to be:  Article 6(1)(e) – ‘...exercise of official authority…’;  And their processing of special categories (health) data using accuRx services, the conditions are expected to be:  9(2)(h) – ‘…health or social care…’, and  9(2)(i) – ‘…public health purposes…’.  For processing special categories (ethnicity) data using accuRx services, the conditions are expected to be:  9(2)(h) – ‘…health or social care…’, and  9(2)(b) – ‘…social protection law…’ (for monitoring equality of access)  Anyone using accuRx for purposes beyond those set out above are likely to be misusing the software and in breach of the terms and conditions. |

|  |
| --- |
| Step 3: Consultation process |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to  consult information security experts, or any other experts? |
| The Covid-19 vaccination programme was planned and executed quickly. The specification for the primary care Enhanced Service was published on the 1st December 2020 and the vaccine booking solution procured and assured by NHS Digital in the following weeks.  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. This has resulted in [improvements and changes](https://www.notion.so/accurx/PUBLIC-Product-improvements-accuBook-vaccine-booking-b53149e6998046ca919e11c2aa01c7cd) that have been set out here, many of which have been put in place to meet information governance needs (such as measures in place to allow practices to check the quality of uploaded patient information).  Both solutions have been designed adhering [to national specifications from NHS Digital](https://gpitbjss.atlassian.net/wiki/spaces/CVPDR/overview?homepageId=2717090030). Both solutions have been assured against these standards, as can be verified on the [NHS Digital website](https://digital.nhs.uk/services/gp-it-futures-systems/assured-appointment-management-solutions-for-primary-care-networks-coronavirus-covid-19-vaccination). It is also built in close alignment to the Enhanced Service specification and other requirements of the vaccine programme., and with flexibility given that the requirements on organisations may change. |

|  |
| --- |
| Step 4: Assess necessity and proportionality |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
| accuRx always acts as a data processor in relation to patients’ data that providers share with accuRx through the use of its software services.  Health care providers’ lawful basis for processing patient data using accuRx services is **expected** to be:  Article 6(1)(e) – ‘...exercise of official authority…’;  And their processing of special categories (health) data using accuRx services, the conditions are expected to be:  9(2)(h) – ‘…health or social care…’, and  9(2)(i) – ‘…public health purposes…’.  For processing special categories (ethnicity) data using accuRx services, the conditions are expected to be:  9(2)(h) – ‘…health or social care…’, and  9(2)(b) – ‘…social protection law…’ (for monitoring equality of access)  Anyone using accuRx for purposes beyond those set out above are likely to be misusing the software and in breach of the terms and conditions.  AccuRx has successfully completed NHS Data Security and Protection Toolkit assurance (under NHS ODS code 8JT17), and both the Cyber Essentials and Cyber Essentials Plus certification. Cyber Essentials is a scheme run by the UK government and the National Centre for Cyber Security to help you know that you can trust your data with a given supplier. AccuRx’s sub-processors operate based on Article 28 GDPR-compliant agreements. AccuRx data is encrypted in transit via HTTPS and [encrypted at rest](https://docs.microsoft.com/en-gb/azure/storage/common/storage-service-encryption) via TDE. AccuRx follow the Microsoft Azure Security and Compliance Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. The company’s latest credentials can be found at <https://www.accurx.com/security-and-privacy/our-resources>.  **Vaccine product**  **Booking solution**  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 are booked into. Sharing across practice boundaries is necessary to support collaborate hub-style models of  **Recording solution**  When a patient vaccination record has been created, it is safeguarded:   * it is handled in line with instructions from the GP practice in line with NHS Digital standards defined by the GP IT Futures framework. * its default retention period will be in line with that for the practices involved to administer the programme, and so it is likely that the Enhanced Service specification’s default end date is the 31st August 2021. NHS Digital guidance will further clarify this. * the vaccination record is saved back to the clinical IT system through a standard route. When accuTrack goes live, this will involve passing the information to NHS Digital’s Data Processing Service, which will ensure saving back to the clinical record as described in the Point of Care Specification . * onward sharing to NHS Digital is done at the instruction of the PCN Grouping under the terms of the collaboration agreement * the information remains accessible and under the control of the practice only (as they are the data controller) |

|  |  |  |  |
| --- | --- | --- | --- |
| Step 5: Identify and assess risks | | | |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| Access to Personal data by persons other than the data subject or legitimate user of the solution | Low | Significant | Low |
| The integrity of the computers used (how at risk are they from trojans or viruses) | Low | Minor | Low |
| Patients impersonating eligible patients in order to receive the Covid-19 vaccine | Low | Low | Low |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step 6: Identify measures to reduce risk | | | | |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| 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 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. | Reduced | Low | Yes |
| The integrity of the computers used | Both solutions can be 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. | Reduced | Low | Yes |
| 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 record corrected, and vaccine administered. | Reduced | Low | Yes |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Step 7: Sign off and record outcomes | | |
| **Item** | **Name/position/date** | **Notes** |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: |  | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | Trudy Slade | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice:  Practices should read and understand the DPIA and need for the data processing in this instance. Personal confidential data, in the form of patient demographic and minimum personal data is shared with other data controllers in their network for the purposes of providing the Covid 19 Vaccine, this process will enable an accurate record of who has had the vaccine and avoid duplications. It will enable other organisations with a contract in place and who is providing recall and booking services to the national vaccine service the ability to target the right patients at the right time according the national role out.  Practices should understand that the records of patients registered at other practices, will be visible to all users of within a shared network.  The practice should update their information Asset register to reflect the use of AccuBook and their data flow map.  The practice should also ensure that they have updated their Privacy notice – suitable wording below   |  |  | | --- | --- | | Covid-19 Mass Vaccination Programme | **Purpose** – The practice will share a minimum of patients personal confidential data in order to book, record and recall patients for their Covid-19 vaccination. It is essential that all patients are offered the vaccine in the interests of Public Health. Patients cannot opt out of the recall system.  **Legal Basis :** While this activity is covered under the COPI regulations, it is also for direct care, and Public interest. All UK GDPR legal basis applicable are listed below.  Health care providers’ lawful basis for processing patient data using accuRx services is expected to be:  Article 6(1)(e) – ‘...exercise of official authority…’;  And their processing of special categories (health) data using accuRx services, the conditions are expected to be:  9(2)(h) – ‘…health or social care…’, and  9(2)(i) – ‘…public health purposes…’.  For processing special categories (ethnicity) data using accuRx services, the conditions are expected to be:  9(2)(h) – ‘…health or social care…’, and  9(2)(b) – ‘…social protection law…’ (for monitoring equality of access)  **Processors:** IPC, AccuRX, other GP practices within the Network, other providers assisting with the Mass Vaccination Role out | | | |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |