|  |
| --- |
| **Data Protection Impact Assessment (DPIA)****AccuRx**  |
| This assessment should be completed as part of the business case for all new information systems and processes which involve the use of personal sensitive data or will significantly change the way in which personal data is handled.  |
| The DPIA should be sent to Caldicott Guardian/*IG Lead/SIRO* for review and approval DPO advice may be useful at any stage, including:* how to complete a particular section of the form
* whether a full DPIA is necessary (Screening section)
* possible measures and safeguards to mitigate risks.

The DPO must review the completed form and advise on whether processing should go ahead. |
| **General Details** |
| 1. | Person completing this assessment: | Name: Helen Kershaw Job Title: Primary Care IG LeadEmail: helen.kershaw@imerseyside.nhs.ukPhone: 0151 317 8386/07780 229165 |
| 2. | Name of the new system/process/project work to be undertaken: | AccuRx – Text Messaging and Video Consultations  |
| 3. | Responsible Lead (name & email address): |  Dr M I KhanMohammed.khan14@nhs.net |
| 4. | Background:(Why is the new system/change required - The purpose and aims of this work) | Patient Communications for healthcare professionals AccuRx is a product embedded into EMIS Web that allows a number of ‘digital’ consultation activities to be undertaken, such as SMS questionnaires (responses are entered as a consultation into the patient record) and Video Consultations.The introduction of a new text messaging (SMS) and Video provider “AccuRx” with which to contact registered patients.As this is a new product/system to the practice, it is important to analyse how it may impact on patient data and the processing of this data.During COVID-19 this will minimise the risk of infected patients visiting the GP Practice and to help maintain routine services whilst keeping staff and patients as safe as possible during the current situationMany consultations that do not need to be conducted on a face to face basis can be done over a normal phone call and that ***video consultation should only be used where there is a need to see the patient, but the patient should not attend the surgery*.** Many patients may not have the technology for such a consultation or be comfortable with participating. |
| 5. | List the main activities of the project: | The use of secure SMS and Video Consultations from Primary Care either from on site or home workingClinical and Non-Clinical staff will, with patient consent, correspond via individual text message (SMS)Clinicians to be able to video call patients |
| 6. | What are the intended benefits: | SMS - More efficient and timely contact with patients and more efficient and timely use of human resources in practice.* Reduction in paper, envelopes, stamps, human resources.
* Reduced room for human error

Video - To minimise the risk of infected patients visiting the practice and to help maintain routine services whilst keeping staff and patients as safe as possible |
| 7. | Date new system, process or work to start:  |  |
| 8. | Information Asset Owners (All system/assets must have Information Asset Owners (IAO). IAO’s will be the Practice Manager or Partner GP *This is the person who takes overall responsibility for this asset, and may do so for several other assets. The IAO is responsible for reporting any breaches that happen with their assets to the SIRO, as well as identifying and mitigating any risks to the asset, and deciding which users have access to it.* | Name: | Dr M I Khan |
| Title: | GP |
| Department: | WVMC |
| Telephone: | 0151 2476399 |
| Email: | Mohammed.khan14@nhs.net |
| 9. | Who is the Information Asset Administrator*The IAA is an operational staff member who has day to day responsibility for ensuring that the asset is secure and that those who should be able to access it are able to do so*. | Name: | Dr A Khan |
| Email: | asrakhan@nhs.net |
| 10. | Date DPIA was completed: |  |
| **DPIA Screening** |
| Screening Questions | Yes/No | Comments |
| 11. | Will the project involve the collection of new information about individuals?  | **Yes**  | Yes responses to sms questionnaires and information obtained via video consultations. |
| 12. | Will the project compel individuals to provide information about themselves?  | **Yes** | Based on consent only, NOT compulsory. |
| 13. | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | **No** |  |
| 14. | Do you propose using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?  | **No** | Data is currently used and sent via post/telephone. AccuRx will be a more effective digital way to communicate. |
| 15. | Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition | **Yes** | New Technology  |
| 16. | Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?  | **Yes** | Just like any consultation |
| 17. | Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. health records, criminal records or other information that people would consider to be particularly private? | **Yes** | Video consultations – these are NOT recorded or stored on any server. It would be possible for these to be recorded by third party tools. This may be done by patients. That is the same as them recording a face to face consultation, which they are entitled to do. There is some restriction around patients use of such recordings beyond their own personal/household activities, but that isn’t related to this product specifically. Data channels for the video consultations are encrypted to reduce the risk of interception. |
| 18. | Will the project require you to contact individuals in ways which they may find intrusive? | **Yes**  | AccuRx allows the GP Practice to contact patient via SMS and hold video consultations only when patient has consented. |
| 19. | Will the project store information using cloud technology? | **No** | All EMIS Web GP Practices are adding documents to cloud storage (AWS S3) as they create, bulk migration of historical documents is ongoing Video consultations – these are NOT recorded or stored on any server |
| 20. | Will the project transfer information outside the European Economic Area (EEA)?  | **No** |  |
| * If you answered **no** to all the questions, you **DO NOT** need to proceed to a full Data Protection Impact Assessment. Save this document to evidence your assessment
* If you answered **yes** to any of these questions, you **DO** need to proceed to a full Data Protection Impact assessment. Complete the following sections and save to evidence your assessment
 |
| **Full Data Protection Impact Assessment**  |
| 21. | Who are the Data Subjects? (e.g. the people whose data will be held/processed in this new system – this may be patients and/or staff) |  Patients Registered at the GP Practice  |
| 22. | What Data Classes will be held on this system (i.e. the actual data fields) split by Personal and Special Category  | The Personal Data, including Special Categories of Personal Data, to be processed under an Agreement with AccuRx and the GP Practice, includes but is not limited to the following data relating to ​**Patients of the Data Controller**​, namely: * ​Patient demographic details (name; date of birth; gender)
* ​NHS number
* ​Mobile phone number
* ​Content of the communications with – or regarding - patients sent via AccuRx
* ​Other types of data that may from time to time be required to provide the Services.

The Personal Data relating to **​health care or social care professionals​** involvedin the Patient’s care to be processed under an Agreement includes, but is not limited to:* ​Name
* ​Email address
* ​Mobile phone number
* ​Content of the communications with – or regarding - patients sent via AccuRx
* ​Other types of data that may from time to time be required to provide the Services.
 |
| 23. | Children (those under 13 years of age) Does the project involve internet services of any kind, with regards to children?  | No. The service is for Adult patient only, who have given consent. |
| 24. | If yes, are you planning to gain and record consent? How will you achieve this?  | N/A |
| 25. | If the child is under 13 years of age, will you gain and record the parents’ consent? If Yes how will you achieve this?  | N/A |
| 26. | Will this system/process include data which was not previously collected? | No |
| 27. | Have you assessed the likelihood of data causing any unwarranted distress or damage to individuals concerned? | YesConsent Based |
| 28. | Is there a legal basis for holding and processing this data? | GDPR - Article 6(1) Lawfulness of processing:**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.**(d) Vital interests:** the processing is necessary to protect someone’s life.**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. **(Official authority)** |
| GDPR - Article 9(2) Processing of special categories of personal data:**(c)** processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; **(Vital Interests)****(h)** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; **(Health or social care(with a basis in law)/(Provision of health)****(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; **(Public Health (with a basis in law))** |
| 29. | Does the system/process include new or amended identity authentication requirements that may be intrusive? | No |
| 30. | What checks have been made regarding the adequacy, relevance and necessity of data used? | Video - Patient details will be checked at point of consent being given to use this technology. Patient in control. |
| 31. | Can the system/process use pseudonyms or work on anonymous data? | No |
| 32. | Can the data subjects opt-out of their data being added to the system/used by the process, and if so is this publicised? | Yes patients can opt out of SMS and Video **Privacy Notices to be updated** |
| 33. | Does the Fair Processing Notice (or Privacy Notice on the practice’s public website cover your planned activity | Yes – **Privacy Notices to be updated** |
| 34. | Who are the partners for the data sharing? | AccuRx (SMS) Whereby(host Video)GP Practice Name  |
| **Data Security** |
| 35. | Will the system require the use of the practice computer equipment? If so has the Informatics Merseyside (IM) IT Security Team been informed and assessed the system?  | Yes for SMS Video - Practices will use a combination of their own equipment and that supplied by IM  |
| 36. | Who will use the system/process and have access to the data? | Clinical and Non-Clinical staff will, with patient consent, correspond via individual text message (SMS)Clinicians to be able to video call patients |
| 37. | Have or will areas involved completed the Data Security Awareness module | Yes – All staff are required to complete Data Security Awareness Level 1 as part of their mandatory training annually |
| 38. | Will the data be shared with any other organisations?(check privacy policy of provider/Sharing Agreements for details) | Only the partners in the Agreements between AccuRx and the GP Practice  |
| 39. | Where will data be held?  | In EMIS Web Data will be held in the Patients Record within EMIS WebSMS – Auto StoredVideo – manually recorded in consultationEMIS Data will be stored in:Fulford Grange, Mickelfield Lane, Rawdon, Leeds, LS19 6BA and Stafford House, Leathley Road, Hunslet, Leeds, LS10 1BGAWS for GP Documents – UK server  |
| 40. | What format will data be stored in? | Data will be held in the Patients Record within EMIS WebSMS – Auto StoredVideo – manually recorded in consultation |
| 41. | Does the system / process change the way data is stored? | No |
| 42. | How will staff access and amend data? | Access will be via EMIS Web, if data is identify any inaccuracy found can be amend by the GP Practice as Data Controller |
| 43. | How will data be shared? e.g. email, NHS mail, internal/external post, phone, website transfer, MESH, SMS | SMS and Video Calls  |
| 44. | Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)? | [ ]  Yes [x]  No*If yes, please outline the data types, flow (sending/receiving), country, transfer methods and any measures in place to ensure adequate levels of security when transferred (in transit)to this country.* |
| 45. | Description of information flows (either words or diagram)  | **SMS** - Data will be drawn from the patient record on Emis. The relevant template will be selected from the AccuRx icon and a text message will be sent to the patient. An automatic “pop up” will appear if the patient has given consent for contact in this way. **Video** Telephone triageConsent gained to use video consultationVia AccuRx website initiate phone callSMS from AccuRx to practice and to patientBoth have to accept the video requestFace to face (screen) consultation. |
| 46. | What security measures have been taken to protect the data? (request 3rd party security whitepapers or documentation for system)Please include access control, data security in transit and encryption in the answer  | **Secure Video Consultation**AccuRx is NHS Digital approved [video consultation supplier](https://digital.nhs.uk/services/future-gp-it-systems-and-services/approved-econsultation-systems). The video consultation service is fully secure and compliant with GDPR and DCB0129. The video and audio communication is only visible to participants on the call and transmitted over an encrypted connection. It is not recorded or stored on any server. The video consultation connection prioritises ‘peer-to-peer’ connections between the clinician’s and patient’s phone and follows NHS best practice guidelines on health and social care cloud security.**Secure Data Processing**AccuRx host their servers in the London Microsoft Azure Data Centre. They follow [best practice guidance](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) from NHS Digital, the UK National Cyber Security Centre (NCSC) and Microsoft. See [here](https://docs.microsoft.com/en-us/azure/security/blueprints/uknhs-paaswa-overview) for detailed information. All data sent is encrypted when in transit (when it is sent) and at rest (when it is stored).**Meeting NHS Standards**AccuRx are an NHS Digital approved [supplier](https://digital.nhs.uk/services/future-gp-it-systems-and-services/gp-it-system-suppliers-awarded-contracts). They have [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/News/34) assurance (ODS code: 8JT17), and have the [Cyber Essentials Plus](https://www.cyberessentials.ncsc.gov.uk/cert-search/?query=accurx) certification. |
| 47. | Is there a useable audit trail in place for the asset? *For example, to identify who has accessed a record* | YesFull audit trails are kept of all user activity for clinical safety purposes.AccuRx records every text sent and by whom in the patient records this includes the video link text.  |
| 48. | How often will the system/process be audited? | **GP Practice to complete** |
| 49. | Who supplies the system/process? | **Walton Village Medical Centre** |
| 50. | Is the supplier of the system/recipient of the data registered with the ICO? (please give registration number) | * AccuRx Limited Registration Number: ZA202115
* **Walton Village Medical Centre** Registration Number: N82668
 |
| 51. | If third party supplier are they based within the EEA  | Yes |
| 52. | Where will the 3rd party store the data? (full addresses)  | No patient or user demographic information is collected or stored by AccuRx or the hosted service (Whereby). |
| 53. | Has the organisation completed the Data Security and Protection (DSP)Toolkit to a satisfactory level?  | Yes, all partners are required to complete the NHS Digital DSP Toolkit and achieve ‘Standards Met’.AccuRx Limited have completed the NHS Digital DSP Toolkit scoring ‘Standards Exceeded’ for year 18/19 submitted on 31/03/2019. (ODS 8JT17) |
| 54. | Does the contract/sharing agreement include necessary IG clauses? | AccuRx has a standard data processor agreement ([https://www.AccuRx.com/data-processing-agreement](https://www.accurx.com/data-processing-agreement)), deemed to be generally in line with the requirements of GDPR article 28 (processors). |
| 55. | What business continuity plans are in place in the case of data loss / damage as a result of human error / computer virus / network failure / theft / fire / flood / other disaster? | Each Partner has its own Business Continuity Plan in place  |
| **Data Quality**  |
| 56. | Who provides the information for the asset? | GP Practice and Patient |
| 57. | Who inputs the data into the system?  | GP Practice and Patient |
| 58. | How will the information be kept up to date and checked for accuracy and completeness? | GP Practice when obtaining consent from patient |
| 59. | Can an individual (or a court) request amendments or deletion of data from the system? | Requests can be made, these will be reviewed on individual basis and if found to be appropriate for amendment/deletion |
| **On-Going Use of Data** |
| 60. | Will the data be used to send direct marketing messages?  | No |
| 61. | If yes, are consent and opt-in procedures in place? | N/A  |
| 62. | Does the system/process change the medium for disclosure of publicly available information? | No |
| 63. | Will the system/process make data more readily accessible than before? | No  |
| 64. | What is the data retention period for this data? *(please refer to* [*Records Management for Health & 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) ) | In line with [Records Management for Health & 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) |
| 65. | How will the data be destroyed when it is no longer required? | In line with NHS Digital Destruction and Disposal of Sensitive Data Good Practice Guidelines  |
| 66. | Does your disaster recovery solution use 3rd party supplier? | no |
| 67. | Please provide details of all accreditations the supplier holds e.g. ISO27001 | AccuRx has the following standards/accreditations:* DCB129 (Clinical safety risk management) – self assessed to NHS Information standard
* NHS Data Security & Protection Toolkit 18/19 – standards exceeded. (Self assessment)
* Cyber Essentials Plus accreditation - p-7197786. Date issued: 29/11/2019
* Information Commissioner Registration - ZA202115
* Firetext (who send SMS on behalf of AccuRx) are ISO27001 certified. They also use BT/EE but their status is currently unclear.
* Data processed by AccuRx is via servers on Microsoft Azure cloud, based in London. Data is encrypted both during transmission and at rest.
 |
| 68. | Has your Disaster Recovery Plan been tested and was all data retained and secure? |  |
| **Identify and Assess Risks**  |
| Information security risks should be highlighted to the IM IT Security Team to complete any necessary risk assessments on new systems or changes to existing systems. Any issues that may arise could adversely impact other organisations and services hosted by Informatics Merseyside, because of this the IM IT Security Team need to complete their assessment before the system can be commissioned for use.  |
| **Risk Description (**source of risk and nature of potential impact **to individuals, the Practice, CCG or to wider compliance)** | **Likelihood of harm**(Remote, possible or probable) | **Severity of harm**(minimal, significant or severe) | **Overall risk**(low, medium or high) |
| Access to Personal data by persons other than the data subject | Remote | Significant  | Low |
| Incorrect patient data selected for SMS | Remote | Significant  | Low |
| Sensitive data being sent via SMS | Remote | Significant  | Low |
| Abusive messages are sent to patients by a user | Remote | Significant  | Low |
| The integrity of the computers used (how at risk are they from trojans or viruses) | Remote | Minimal | Low |
| The clinician would need to ensure that there was no third-party data visible on desks or screens that could be viewed or captured by the individual in any video call | Remote | Minimal | Low |
| A third party is present in the room of one of the video consultation participants without the other participant knowing | Remote | Significant  | Low |
| A third party guesses the URL of a video consultation and joins the call | Remote | Minimal | Medium |
| **Identify Measure to Reduce Risk** |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in the table above** |
| **Risk** | **Proposed Risk Solution** (reduce or eliminate risk) | **Effect on risk**(Is the risk reduced, transferred, accepted) | **Remaining risk**(Low, medium or high) | **Measure approved**(Yes/No) |
| Access to Personal data by persons other than the data subject | Users are authenticated by requiring: NHSmail to register for an account; 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 EMIS Web principal care systems. This ensures that a user can only access data of patients registered at their practice. Any video consultations are not recorded or stored. | Eliminated  | Low  |  |
| Incorrect patient data selected for SMS | Patient demographic data is only pulled from EMIS Web principal care systems. This ensures that a user can verify the correct information with the patient before sending an SMS.Users have to  agree to an acceptable use policy that includes confirming that the service not be used to communicate SMS messages that are sensitive or clinically urgent messages. Where a link to sensitive data is shared (e.g. to a document), the patient has to verify their identity by typing in the date of birth. | Reduced  | Low |  |
| Sensitive data being sent via SMS | Users have to agree to an acceptable use policy that includes confirming that the service not be used to communicate SMS messages that are sensitive or clinically urgent messages. Full audit trails are kept of all user activity for clinical safety purposes. | Reduced  | Low |  |
| Abusive messages are sent to patients by a user | AccuRx scans SMSs for abusive content and flags to its Clinical Lead if any are detected.Full audit trails are kept of all user activity for clinical safety purposes. | Reduced  | Low |  |
| The integrity of the computers used (how at risk are they from trojans or viruses) | Use of devices that comply with NHS standards of encryption. | Reduced  | Low |  |
| The clinician would need to ensure that there was no third-party data visible on desks or screens that could be viewed or captured by the individual in any video call | Clinicians can view what the patient views in the video consultation. Therefore, any third-party data could be identified and blocked by the clinician. | Reduced  | Low |  |
| A third party is present in the room of one of the video consultation participants without the other participant knowing | Participants can ask the other participant to scan the room with the camera if either are concerned.  | Reduced  | Medium |  |
| A third party guesses the URL of a video consultation and joins the call | Each URL generated is completely unique, rendering it almost impossible to guess by a third party. They would also have to guess it at precisely the same time other participants are in the virtual meeting room. Even if they did both of those (incredibly unlikely) things, participants can immediately see when another participant joins the call and end the call.  | Eliminated  | Low |  |
| **DPIA Sign Off** |
| Item | Name/Date | Notes  |
| SIRO approved: | Name:Dr M I Khan | *Integrated actions back into project plan, with date and responsibility for completion* |
| Date: 02/05/2020 |
| Caldicott Guardian approved:  | Name: Dr M I Khan | *If accepting any residual high risk, consult the ICO before going ahead* |
| Date:02/05/2020 |
| DPO advice provided  | Name:Dr M I Khan | *DPO should advise on compliance, Identify measure to reduce risk section and whether processing can proceed* |
| Date: 02/05/2020 |
| Summary of DPO advice:  |
| DPO advice accepted or overruled by:(SIRO/Caldicott Guardian) | Name: | *If overruled, you must explain your reasons* |
| Date: |
| Comments: |
| Consultation responses reviewed by: | Name: | *If your decision departs from individuals’ views, you must explain your reasons* |
| Date: |
| Comments: |
| This DPIA will be kept under review by: | Name: | *The DPO should also review ongoing compliance with DPIA* |
| Date: |

**Additional Information can be found via the following;**

AccuRx Privacy Policy: <https://www.accurx.com/privacy-policy>

AccuRx Security: <https://www.accurx.com/security>

AccuRx Chain(SMS) sample DPIA: <https://docs.google.com/document/d/1koOA8L2gE6SCD21IUsVmfy0sLsS7OGn7fEfYb_byijI/edit?ts=5e6f7e35>

AccuRx Video sample DPIA: <https://docs.google.com/document/d/1Q7WgTiuIG8ikkKCg6uiLxuSWodfX4955XM-TVN6mYJg/edit>

AccuRx GDPR Questions: <https://www.accurx.com/gdpr-questions>

NHS Digital Approved Video Consultation Systems:

<https://digital.nhs.uk/services/future-gp-it-systems-and-services/approved-econsultation-systems>

Whereby Security Info

https://whereby.helpscoutdocs.com/category/382-account-and-privacy