Doc Abode Data Protection Impact Assessment

Section 1: Background Information

Project Name:	**Doc Abode**
Organisation	Doc Abode ltd.
Assessment Completed By	Phil Walker
Job Title	Data Protection Officer
Phone	07388 340416
E-mail	pdwalker87w@btinternet.com

Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required.

The Doc Abode software platform supports NHS healthcare providers to deliver more responsive, cost-effective care by safely connecting and matching a multi-disciplinary clinical workforce to NHS patient needs, in real-time, based on availability, proximity and expertise. It aims to accomplish this through the introduction of a platform incorporating a mobile application for use by HCPs to engage a flexible workforce to carry out home visits outside of a regular shift rota. Providing greater capacity for home visits, enabling better matching of location and speciality to each visit, and creating preferably working patterns for more HCPs. Ultimately Doc Abode intends to use predictive analytics combined with artificial intelligence. Doc Abode facilitates attracting a 'new' workforce from clinicians disengaged with traditional ways of working. Funding was received from Yorkshire & Humber Academic Health Science Network (AHSN) and the Small Business Research Initiative.

Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.

In the previous existing LCD operational model, urgent care home visits were predominantly staffed by GPs who are highly skilled. However the workforce pool is limited and this means that, during periods of high demand, it can lead to variable operational costs and response times.

In the traditional operating model, GPs are driven to patients requiring home visits in one of LCD's dedicated cars. Through its innovative digital platform, which facilitated a new way of working, the goal of Doc Abode was three fold:

- To improve the clinical outcomes of urgent care patients by improving response times.
- To increase the total available workforce by providing an alternative to the traditional shift based way of working.
- To improve the operational efficiency of deployment of clinicians by matching the nearest clinician, with the right skills set, with availability to an urgent care home visit, in real-time.

Information that is collected which falls into these following purposes:

1. Clinical risk management to verify and authorise who may use the system – Only those who are clinically approved through a defined process may use the system. Information is also collected on HCP preferences. This information is collected via the 'Onboarding' application. A limited subset, is transferred to the 'operational application'.

2. Patient identifiable information which is transferred into the 'operational application' from other patient management systems for use by the HCPs for patient treatment.

3. Operational Data - Operational data is collected via the 'operational application' which is used for deploying HCPs to patient jobs (ie home visits) by 'operators'. Operational data is also collected from the mobile app used by HCPs. Operators work for the healthcare organisation and issue jobs to HCPs. HCPs optionally decide which jobs to accept and then undertake these jobs following a specific workflow utilising a mobile app. This data is also used for operational monitoring for KPIs such as speed of response to a patient. In time it is expected that this data will also provide the baseline information to provide to an 'Artificial Intelligence' engine to improve the matching of HCPs to patient requirements.

4. Audit Data – data from the operational system is captured into a separate audit database.

5. Evaluation Data – this will be collected from the 'operational application' back end database (note data from the mobile app is collected at the backend database). Also some non-patient identifiable data may be collected from the SystmOne out of hours module. Evaluation data will be used for research purposes, and also for Management Information purposes to monitor the use of the system. This is covered through appropriate Information Sharing Agreements with the provider.

Information pertaining to the patient is already captured through 111 and stored in other systems. The impact to the patient is that this data will be transferred into the Doc Abode system specifically for the execution of the Doc Abode home visit, and only stored within Doc Abode for the time required to carry out this primary purpose and satisfy audit requirements. This means that their data is held by an additional Data Processor organisation and stored in additional infrastructure. This increases the number of places where a data security breach could potentially occur. However it does not increase the extent of the data held about the patient nor employ it for purpose other than the home visit that the patient has already consented to.

Information pertaining to the HCP will be held in order to positively authenticate them as users of the system, for the out of hours provider organisation to approve them for carrying out home visits, thus protecting patient data, and for the purposes of ensuring the most appropriate jobs are offered to them. Demographic and geographical information is held in relation to the HCP but not more sensitive data such as healthcare records.

Provide details of any previous DPIA or other form of personal data compliance assessment done on this initiative.   If this is a change to an existing system, a DPIA may have been undertaken during the project implementation

An NHS IG Toolkit assessment was undertaken for 2017/18 and a minimum satisfactory score of 66% was reported (Level 2 accredited).

Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change.

The following functions/stakeholders are affected by the system, in the data management sense (please also refer to the 'Doc Abode Data Flows' diagram enclosed):

1. Patients data will be stored in the new system and they will receive care from HCPs determined via the new Doc Abode process and system. The patient experience should remain the same whilst response times should improve.

2. Health Care Professionals (HCP) provide evidence of qualifications, clinical checks, and references in order to be authorised by healthcare organisations. The software for this has been written by an organisation called Synap. HCPs also use Mobile App software – for use on Apple iPhones and Android phones to be alerted about potential jobs, to accept those jobs, and then to complete the jobs under a specific workflow. The software has been written by an organisation called BJSS.

3. Healthcare organisations use the Doc Abode application to verify the credentials of HCPs and for operationally deploying home visits to patients by Health Care Professionals (HCPs). The software has been written by an organisation called BJSS.

Section 2: The Data Involved

There are two types of data collected – Patient and HCP. Each is considered separately in this section.

Patient Data	Data Type		Justifications
Information that identifies the individual and their personal characteristics	Name	☒	Obviously medical condition, identity, contact and location data are essential for providing the service. Other data items may be relevant in some circumstances but will not be recorded where not.
	Address	☒	
	Postcode	☒	
	Dob	☒	
	Age	☒	
	Sex	☒	
	Gender	☒	
	Racial/ethnic origin	☒	
	Physical description	☐	
	NHS no.	☒	
	Mobile/home phone no.	☒	
	Email address	☒	

	Yes	N/A	Justification
Information relating to the individual's physical or mental health or condition	☒	☐	Required to assess required care
Information relating to the individual's sexual life	☒	☐	May be relevant in some circumstances but will not be recorded where not.
Information relating to the family of the individual and the individuals lifestyle and social circumstances	☒	☐	May be relevant in some circumstances but will not be recorded where not.
Information relating to any offences committed or alleged to be committed by the individual	☐	☒	
Information relating to criminal proceedings, outcomes and sentences regarding the individual	☐	☒	What about risk flags? May be relevant in some circumstances but will not be recorded where not.
Information which relates to the education and any professional training of the individual	☐	☒	
Employment and career history	☐	☒	
Information relating to the financial affairs of the individual	☐	☒	
Information relating to the individual's religion or other beliefs	☒	☐	May be relevant in some circumstances but will not be recorded where not.
Information relating to the individual's membership of a trade union	☐	☒	

HCP Data	Data Type		Justifications
Information that identifies the individual and their personal characteristics	Name	☒	**This information is captured as part of the onboarding process if the HCP wishes to register for Doc Abode. These details are accessible to the provider organisation to enable them to certify and authentic their suitability to undertake work on the Provider's behalf. Doc Abode does not provide the assurance for the HCPs. The providers can access the HCP data through secure login credentials to the onboarding platform.**
	Address	☒	
	Postcode	☒	
	Dob	☒	
	Age	☒	
	Sex	☒	
	Gender	☒	
	Racial/ethnic origin	☐	
	Tel no.	☒	
	Physical description	☐	
	NHS no.	☐	
	Mobile/home phone no.	☒	
	Email address	☒	

	Yes	N/A	Justification
Information relating to the individual's physical or mental health or condition	☒	☐	
Information relating to the individual's sexual life	☐	☒	
Information relating to the family of the individual and the individuals lifestyle and social circumstances	☐	☒	
Information relating to any offences committed or alleged to be committed by the individual	☐	☒	
Information relating to criminal proceedings, outcomes and sentences regarding the individual	☐	☒	
Information which relates to the education and any professional training of the individual	☒	☐	Must be captured about the HCP as part of on boarding process to carry out the necessary checks to ensure they are suitable for carrying out the work and to safeguard the patient.
Employment and career history	☒	☐	Must be captured about the HCP as part of on boarding process to carry out the necessary checks to ensure they are suitable for carrying out the work and to safeguard the patient.
Information relating to the financial affairs of the individual	☒	☐	Limited financial data including bank account and pay rate
Information relating to the individual's religion or other beliefs	☐	☒	
Information relating to the individual's membership of a trade union	☐	☒	

Section 3: Assessment

	Question	Patient	HCP
Legal compliance – is it fair and lawful?	1. What is the legal basis for processing the information? *This should include which conditions for processing under the GDPR apply and how the common law duty of confidentiality will be met.*	Processing is in the legitimate interests of the organisations involved. Processing of special category data is for medical purposes under clinical direction. Patient consent is required under common law but can be implied for care purposes.	Processing is in the legitimate interests of the organisations involved. No data on HCPs is held in confidence.
	2. a - Is the processing of individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act? b - Have you identified the social need and aims of the initiative and are the planned actions a proportionate response to the social need?	There is no interference with the right to privacy as identifiable data is only used to support care and the approach adopted is a proportionate response to satisfying the identified need for timely and effective care provision.	HCPs who register with Doc Abode work under contract to the CCG **[Is that right?]** and by signing the contract agree to the required processing of data.
	3. It is important that individuals affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed?	Doc Abode provides a privacy notice that covers the processing it undertakes but primary responsibility rests with the data controllers who use Doc Abode's services.	
	4. If you are relying on consent to process personal data under the GDPR, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?	Consent is not required under GDPR as the process relies upon a different legal basis. Consent under common law is implied.	Consent is not required under GDPR as the process relies upon a different legal basis. Consent is not required under common law as none of the data held on HCPs is confidential.
Purpose	5. Does the project involve the use of existing personal data for new purposes?	No, the data provided by patients seeking care is new data. Any access to existing data is for care purposes, a new process but not a new purpose.	No. The data collected through the onboarding process is new.
	6. Are potential new purposes likely to be identified as the scope of the project expands?	No. Personal data will not be used for other purposes. Any new purposes will be supported by anonymised data.	
Adequacy	7. Is the information you are using likely to be of good enough quality for the purposes it is used for?	Yes. Information is entered specifically for this purpose by NHS 111 and triage is carried out by urgent care Operators. Insufficient data can be flagged and corrected at	Yes. Information is added by HCPs themselves at the onboarding stage. This is checked and verified by the healthcare organisation accepting the registration.

		numerous stages before a job is entered into the Doc Abode system.	
Accurate and up to date	8. Are you able to amend information when necessary to ensure it is up to date?	Yes, operators may edit existing jobs in the system.	HCPs may edit information held about them through the onboarding process.
	9. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	This is the responsibility of the healthcare organisations that utilise Doc Abode's services. However, patients are generally treated by the NHS as they present without checks.	HCP data is verified by the healthcare organisations that contract with Doc Abode for its services.
Retention	10. What are the retention periods for the personal information and how will this be implemented?	In line with the NHS Digital Records Management CoP for patient data that is not integral to the clinical record data will be held for a minimum of 3 years and will then be reviewed.	HCP data will be held for the period that the HCP is registered with Doc Abode plus 3 years to allow resolution of any subsequent serious incidents, complaints and outstanding contractual matters.
	11.Are there any exceptional circumstances for retaining certain data for longer than the normal period?	Potentially to resolve litigation or professional investigations	
	12. How will information be fully anonymised or destroyed after it is no longer necessary?	Please see https://aws.amazon.com/s3/faqs/ And https://aws.amazon.com/blogs/security/aws-obtains-iso-27018-privacy-certification/	
Rights of the individual	13. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held?	See the Doc Abode Subject Access Policy [Does this exist?]	
Appropriate technical and organisational measures	14. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?	All Doc Abode staff and operational support staff undertake mandatory IG training. Doc Abode client staff are responsibility of their own organisations. Doc Abode's clients are responsible for ensuring the HCPs provided with patient data have undergone IG training.	All Doc Abode staff and operational support staff undertake mandatory IG training.
	15. If you are using an electronic system to process the information, what security measures are in place?	Security best practices for AWS Cloud infrastructure have been applied and the system will have been independently Penetration tested. (See additional documentation.)	

	16. How will the information be provided, collated and used?	Patient data is provided by administration systems operated by the healthcare organisations that have contracted with Doc Abode. Limited data is made available to HCPs who may choose to accept a job with more information available to those who accept. Data may rarely be accessed by Doc Abode technical staff to fix issues.	HCP data is provided directly by HCPs via the onboarding process. It is used to register a HCP to deliver care via the Doc Abode system and, in time, will use interests, experience and specialties to inform patient allocation. Healthcare organisations verify HCP qualifications.
	17. What security measures will be used to transfer the identifiable information?	All application data, whether identifiable information or not is encrypted in transit through the use of technology such as HTTPS (TLS).	
Transfers both internal and external including outside of the EEA	18. Will individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?	Personal information will be disclosed to the HCP in order for them to carry out the job, this will be done securely through the mobile application. In certain circumstances Doc Abode'soperations staff may need to accesspersonal information through the audit data in order to diagnose an issue. Access to the production system will be strictly controlled and audited through Identity Access Management (IAM) and Role Based Access Control (RBAC). The individuals will have carried out security training and read and acknowledged Doc Abode security policy. Only authorised personnel will be able to access data held in Production systems and they may only do so if they have legitimate reason.	In certain circumstances Doc Abode's operations staff may need to access personal information through the audit datain order to diagnose a system issue. Access to the production system will be strictly controlled and audited through Identity Access Management (IAM) and Role Based Access Control (RBAC). The individuals will have carried out security training and read and acknowledged Doc Abode security policy. Only authorised personnel will be able to access data held in Production systems and they may only do so if they have legitimate reason.
	19. Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data?	No	Yes, this is supported by HCP consent obtained via acceptance of our Privacy Policy which states that we use a 3rd party tools such as Segment to track key user information and events. The data is therefore transferred to the U.S. under the EU/US privacy shield . From Segment, data is then sent to Intercom . Intercom

		is what Doc Abode uses to provide & administer support to users throughout the onboarding process. A Google pixel is also used on our website to attribute conversions / ad campaigns.
Consultation	20. Who should you consult to identify the privacy risks and how will you do this? Identify both internal and external stakeholders. *Link back to stakeholders on page 3.*	Privacy risks have been considered by an information governance steering group in the preparation of a draft DPIA. The draft will be shared with data controllers to establish whether there are any additional privacy risks that have not been considered.
	21. Following the consultation – what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc.	TBC
Guidance used	22. List any national guidance applicable to the initiative that is referred to.	NHS Digital – NHS and Social care data: off-shoring and the use of public cloud services. NCSC - Implementing Cloud Security Principles ICO GDPR guidelines Confidentiality: NHS CoP

-