

**Introduction**

The Data Protection Impact Assessment (DPIA) is for the use of mobile ECG device (AliveCor) in Humber Teaching NHS Trust GP Practices. The DPIA has been completed by the National Lead for the Atrial Fibrillation (AF) Programme.

The DPIA was approved by the IG Group in December 2018.

Privacy Impact Assessment Template

Section 1: Background Information

|  |  |
| --- | --- |
| Project Name: Mobile ECG device roll out |  |
| Organisation Lancashire Care Foundation Trust acting as host for the Innovation Agency Academic Health Science Network |  |
| Assessment Completed By |  |
| Job Title.  AF Programme manager, AHSN Network |  |
| Date completed 29/11/2017 |  |
| Phone |  |
| E-mail |  |
| 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. | |
| Atrial fibrillation (AF) is the most common sustained cardiac arrhythmia.[[1]](#footnote-1) The prevalence of AF in England is likely to be close to 2.0%, which equates to about 835,000 people living with the condition. If left untreated atrial fibrillation is a significant risk factor for stroke and other morbidities.[[2]](#footnote-2) People with AF have a higher prevalence of heart failure, myocardial infarction, hypertension, angina and diabetes and AF is associated with a 5‑fold increase in the risk of stroke.1  AF may have non-specific symptoms or no symptoms at all. It is often only diagnosed following serious complications including stroke, thromboembolism and heart failure. The NICE guideline on atrial fibrillation states that assessing for an irregular pulse in patients presenting with certain symptoms, and performing an ECG for all patients in whom an irregular pulse has been detected, can detect AF before serious complications develop.1,2  Mobile ECG devices were highlighted by Simon Stevens at NHS Confed 2016 as an area for NHS innovation. NHS England has identified funding to help stimulate the market and increase the uptake to innovative mobile ECG technologies in primary and community care.  The Innovation Agency will use the funding to purchase mobile ECG technology that can be used to detect AF in the community, on behalf of all Academic Health Science Networks (AHSNs) and they will lead the allocation and distribution of devices across participating AHSNs. A range of mobile ECG device types will be available through this project (these have met the product specification laid out by NHS England). They are: Kardia by Alivecor, MyDiagnostick, WatchBP, Rhythm Pad by CardioCity, Impulse. The only device which holds data outside the device is Kardia, which operates through a mobile application (app) which is downloaded to a smart phone or tablet.  Each AHSN has identified suitable sites for distribution based on the agreed device allocations (defined from population statistics). Each AHSN will monitor use of the devices and provide implementation support. They will work with an evaluation team to ensure the effective data collection and dissemination of learning. The national AHSN AF steering group will oversee progress. Kardia Mobile is the only device which works with an app and has ECG traces stored by Alive Cor and this will be the focus of the PIA. | |
| 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. | |
| The purpose of this project is to use Mobile ECG technology to facilitate more opportune and timelier detection of AF in primary care. This project has provided the AHSNs with the potential to collectively demonstrate their value, not just in supporting the distribution of these devices, but also by rigorous capture of their use and impact in clinical practice.  The objectives (as specified by the evaluation questions identified by NHS England), include:   * What environments are the devices most effective in? * What features of the implementation packages are most effective? * What impact has the programme had on the market place? * What health economic aspects has the programme achieved? * What impact has the programme had on providers? * What impact has the programme had on patient outcomes? * What is the impact on providers? | |
| What is the purpose of collecting the information within the system? For example patient treatment, patient administration, research, audit, reporting, staff administration etc. | |
| Introducing mobile ECG device technology into a clinical pathway creates the requirement for data to be collected on the outcome for 2 purposes.  For the purpose of clinical record keeping and to facilitate onward referral if required.  To demonstrate the impact of the use of mobile ECG technology in the detection of AF. This data will allow the evaluation team and AHSNs to answer the objectives outlined in the business case. | |
| What are the potential privacy impacts of this proposal - how will this change impact upon the data subject? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing. | |
| Kardia Alivecor:  This device works with the Kardia smartphone app, the privacy statement for which can be found at <https://www.alivecor.com/privacy/en/> .  Kardia - A health care professional (HCP) will download the app to their own or NHS smart-phone or tablet device. In doing so they accept the terms and conditions and enter their NHS.net email address, they should also switch off the voice recording function within the app. We advise that they do not enter any personal or biometric information into the app.  When taking a patient’s ECG trace HCPs should use the “Guest EKG” function and never enter any patient identifiable information (PID) or voice recording to associate with the trace. This will ensure that the patient trace has no identifiable features when it is stored by Alive Cor.  Privacy impact:  The Kardia app for new users has a ‘basic’ and a ‘premium’ (paid for - £10 monthly) version. The premium version is available free for the first month. The basic app allows the recording of a single ECG trace, which is not stored locally or online; whilst the premium service allows the user to store ECG traces locally (on the mobile phone or tablet device) and within a web-based version of the app which can be accessed online.  Risks:  Premium app is provided for free for the first 30 days, therefore users will be required to delete all traces from the journal (i.e remove them from local storage on the app) and to follow the guidance (not adding any PID to the trace). Or should not use the app during this 30 day period. We advise ignoring the premium function.  Transfer of data:  Alivecor collect and monitor usage data on all traces taken such as human ECG data, including the ECG measurement itself, mobile device accelerometer data, average heart rate, the location on the body where the ECG recording was taken (e.g. hand or chest), local time, time zone and geographic location of ECG acquisition. If any PID or voice recording is added to a trace this will also be shared (we advise against this in the guidance).  The data server for European customers is located in the Republic of Ireland. Any user data that leaves the EU is de-identified, complying with EU medical device regulations. | |
| Provide details of any previous Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a PIA may have been undertaken during the project implementation | |
| The AHSN Network has developed a guidance document for the use of mobile devices. This includes guidance recommends the use of the basic app as outlined above. | |
| 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. | |
| NHS England  Lancashire Care Foundation Trust  Academic Health Science Networks  Recipient organisations (for example, CCGs, GP’s, clinical primary care teams) | |

Section 2: The Data Involved

|  |  |  |  |
| --- | --- | --- | --- |
| What data is being collected, shared or used?  (If there is a chart or diagram to explain attach it as an appendix) | | | |
|  | Data Type | | Justifications – there must be justification for collecting the particular items and these must be specified here – consider which data items you could remove, without compromising the needs of the project? |
| Information that identifies the individual and their personal characteristics | Name |  | The HCP who installs the app on their mobile phone/tablet device will be required to add this information. This information is not collected about the patient as they are considered a “guest” when the app is in use.  Should a patient set up the Kardia app on their own device they would be accepting the terms and conditions of the App, which outlines how the data is stored. This is not advised under this roll out.  The employer of the HCP is the Data Controller for this process not LCFT or AHSN, and that the “name” will be the EKG Guest mode |
| 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 |  |  | Data collected from the use of the Kardia device includes human ECG data, including the ECG measurement itself, mobile device accelerometer data, average heart rate, the location on the body where the ECG recording was taken (e.g. hand or chest), local time, time zone and geographic location of ECG acquisition. |
| 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 |  |  |  |
| Employment and career history |  |  |  |
| Information relating to the financial affairs of the individual |  |  |  |
| 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 | Response | Required Action  E.g. Seek Information Governance advice |
| Legal compliance – is it fair and lawful? | What is the legal basis for processing the information? *This should include which conditions for processing under the Data Protection Act 1998 apply* *and the common law duty of confidentiality.* | Health care purposes and medical research |  |
| 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? | No  Yes |  |
| 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? | Consent to take an ECG with the device will be taken by the health care professional in the usual way as with performing any test in the context of healthcare. | No additional consent is needed if the transferred is anonymised |
| If you are relying on consent to process personal data, 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? | This will be in keeping with carrying out medical tests in the course of a consultation. Data will be stored anonymously and therefore could not be accessed if patients wanted to remove it. If permission for the test is not granted it will not be performed. No additional consent is needed. |  |
| Purpose | Does the project involve the use of existing personal data for new purposes? | No |  |
| Are potential new purposes likely to be identified as the scope of the project expands? | No |  |
| Adequacy | Is the information you are using likely to be of good enough quality for the purposes it is used for? | Yes |  |
| Accurate and up to date | Are you able to amend information when necessary to ensure it is up to date? | No |  |
| How are you ensuring that personal data obtained from individuals or other organisations is accurate? | Kardia provides an initial diagnostic test to confirm a diagnosis the patients would be referred for a 12 lead ECG |  |
| Retention | What are the retention periods for the personal information and how will this be implemented? | It is anonymous, but the trace can be emailed to the clinician for inclusion into the clinical record |  |
| Are there any exceptional circumstances for retaining certain data for longer than the normal period? | N/A |  |
| How will information be fully anonymised or destroyed after it is no longer necessary? | <https://www.alivecor.com/privacy/en/> outlines how the data is processed and stored securely.  Data is anonymised as per guidance given to the HCP. No PID is associated with the trace before it goes into the clinical record (if an abnormality is found). |  |
| Rights of the individual | How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held? | No PID will be held.  Removal of data from the Kardia app this will be in accordance with the Alivecor privacy policy  <https://www.alivecor.com/privacy/en/> |  |
| Appropriate technical and organisational measures | What procedures are in place to ensure that all staff with access to the information have adequate information governance training? | Guidance on using the device will be given to all recipients of Kardia.  Devices will be given to HCPs who are required to comply with NHS information governance standards |  |
| If you are using an electronic system to process the information, what security measures are in place? | System securities and only non-personal data is being transferred |  |
| How will the information be provided, collated and used? | By HCP from a patient, Aggregated outcome data will be collected as part of the evaluation. |  |
| What security measures will be used to transfer the identifiable information? | How data is stored is outlined here <https://www.alivecor.com/privacy/en/>  Alive cor use Amazon Web services to host their data cloud. AWS maintains certification with robust security standards, such as [ISO 27001](https://aws.amazon.com/compliance/iso-27001-faqs/), [SOC 1/2/3](https://aws.amazon.com/compliance/soc-faqs/) and [PCI DSS Level 1](https://aws.amazon.com/compliance/pci-dss-level-1-faqs/). AWS is responsible for the security of the underlying Cloud infrastructure (Security of the Cloud) and Alive Cor is responsible for the security of their data and applications (Security in the Cloud). AWS has teams of Solutions Architects, Account Managers, Consultants, Cloud Security Best Practices are followed. |  |
| Transfers both internal and external including outside of the EEA | Will individual’s personal information be disclosed internally/externally in identifiable form and if so to who, how and why? | No, it will only be used in an identifiable form as part of the clinical record |  |
| 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? | N/A |  |
| Consultation | 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.* | The Innovation Agency (hosted by Lancs Care) is responsible for the distribution of the Kardia devices (the project is funded by NHS England). Distribution will be made through the 15 AHSNs. Risks have been discussed with all these parties and specific IG advise sought from Lancashire Care who have supported this guidance and IG lead at Guys and St Thomas’ Foundation Trusts. |  |
| 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. | Issues which have been raised are: the transfer of PID - Guidance issued to mitigate this and the transfer and storage of anonymous data outside the NHS (on Amazon Web servers. |  |
| Guidance used | List any national guidance applicable to the initiative that is referred to. | https://www.england.nhs.uk/publication/nhs-england-innovation-and-technology-tariff-2017-to-2019-technical-notes/ |  |

Section 3 – Privacy issues identified and risk analysis

Identify the privacy and related risks (see Appendix 1 for further information)

*Nb. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column*

*Table 1*

| Ref No. | Privacy issue – element of the initiative that gives rise to the risk | Risk to individuals *(complete if appropriate to issue or put not applicable)* | Compliance risk  *(complete if appropriate to issue or put not applicable)* | Associated organisation/corporate risk *(complete if appropriate to issue or put not applicable)* |
| --- | --- | --- | --- | --- |
| *PR1* | *Individuals are not aware that their data is being processed and held outside the NHS* | *Individuals not aware that their data is being held outside the NHS by a third party* | *Non-compliance with DPA principle 1 – fair and lawful processing* | *May lead to public mistrust*  *May lead to negative view of technology and NHS* |
| PR2 | HCP do not adhere to guidance and add PID to their ECG readings | Identifiable data is being held outside the NHS, which has not been discussed with the individual | *Non-compliance with DPA principle 1 – fair and lawful processing* | *May lead to sanction by the Information Commissioners office (ICO)*  *May lead to legal challenge*  *May bring programme AHSN and NHS E into disrepute*  *May lead to public mistrust* |

Identify the privacy solutions

*Table 2*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ref No. | Risk – taken from column (a), (b) and/or (c) in table 1. | Risk score – see tables at Appendix 2 | | | Proposed solution(s)  /mitigating action(s) | Result: is the risk accepted, eliminated, or reduced? | Risk to individuals is now OK?  Signed off by? |
| Likelihood | Impact | RAG status |  |  |  |
| *PR1* | *Individuals not aware that their data is being held outside the NHS by a third party.*  *Non-compliance with DPA principle 1 – fair and lawful processing*  *May lead to public mistrust*  *May lead to negative view of technology and NHS* | 1 | 4 |  | *Guidance to be developed and implemented by AHSNs to ensure that all recipients of Kardia mobiles are aware of discussing this with patients. Information is made available to patients about how their data is stored. Implementation of this will be overseen by the Community of practice and steering group.* | *Reduced to an acceptable level (it is not possible to eliminate at this stage as the Guidance and implementation will need to ensure it addresses all aspects to enable individuals to be fully informed.* | *Lancashire Care IG lead*  *AHSN National IG Steering Group*  *Risks will be assessed regularly, with feedback from AHSNs* |
|  | HCP do not adhere to guidance and add PID to their ECG readings  Identifiable data is being held outside the NHS, which has not been discussed with the individual  *Non-compliance with DPA principle 1 – fair and lawful processing*  *May lead to sanction by the Information Commissioners office (ICO)*  *May lead to legal challenge*  *May bring programme AHSN and NHS E into disrepute*  *May lead to public mistrust* | 1 | 5 |  | This will be mitigated by:  Production and implementation of guidance  Training provided with the guidance  Internal organisation IG training  Advising the organisation who employs the individual of the project and this issues involved  Communication provided in the environment on using the devices |  |  |

Integrate the PIA outcomes back into the project plan

*NB. This must include any actions identified in Table 1 and Table 2.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Who is responsible for integrating the PIA outcomes back in to the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future? | | | | | | | |
| Ref No. | Action to be taken | Date for completion of actions | Anticipated risk score following mitigation | | | Responsibility for action – *job title not names* | Current status/progress |
| Likelihood | Impact | RAG status |
| *PR1* | *Guidance is developed* | *December 2017* | *1* | *2* |  | *Project Manager to develop guidance and communication for data controllers and users of the App* | *Guidance is developed and communication in progress. All AHSN leads are tasked with implementing this when they distribute the devices* |
| PR2 | Sign off and agreement  Governance process | December 2017 | 1 | 3 |  |  |  |
|  |  |  |  |  |  |  |  |

**Kardia mobile data Flow map**



Appendix 2

1. 1 NICE Medtech innovation briefing [MIB35] [AliveCor Heart Monitor and AliveECG app (Kardia Mobile) for detecting atrial fibrillation](https://www.nice.org.uk/advice/mib35/chapter/Introduction). published date: August 2015 [↑](#footnote-ref-1)
2. 2 NICE Clinical guideline [CG180] [Atrial fibrillation: management](https://www.nice.org.uk/guidance/cg180/chapter/Introduction). Last updated: August 2014

   Please see <https://www.nice.org.uk/guidance/cg180/chapter/1-Recommendations#diagnosis-and-assessment> for more information [↑](#footnote-ref-2)