Action notes

GP Data Patient and Public Engagement and Communications Advisory Panel

Date: Thursday 24 November 2022

Time: 09:30am to 11:00am

Location: MS Teams dial in

Time	Agenda Item	Owner
9:30	Introductions	**Grace Melvin**
9:35	Formal noting of previous meeting's action notes	**Grace Melvin**
09:45	Showcase of NHS Digital's Secure Data Environment	**NHS Digital SDE team reps**
10:30	Comfort break	
10:35	In-person meeting discussion	**Grace Melvin**
10:55	Any other business	**Grace Melvin**

Attendees	Organisation
Grace Melvin (CHAIR)	Association of Medical Research Charities (AMRC)
Eileen Phillips	National Data Guardian
David Snelson	use MY data
Lay member	Lay member
Lay member	Lay member
Lay member	Lay member
Lay member	Lay member
Lay member	Lay member
Assistant Head of Communications	NHS Digital
Communications and Stakeholder Engagement Manager	NHS Digital
Business Support	NHS Digital
SDE team	NHS Digital
SDE team	NHS Digital
SDE team	NHS Digital

Action notes

Apologies	Organisation
Lay member	Lay member
Lay member	Lay member
Lay member	Lay member
Lay member	Lay member
Rebecca Moore	Healthwatch

Agenda item	Notes
1.	**Introductions** Panel members were welcomed to the meeting by the Chair, who also ran through the agenda. Apologies were noted. Further to the discussion on GP Data – commercial arrangements & data flows beyond the NHS in the previous meeting, it was noted that there will be a presentation from the National Data Guardian on the topic at a future meeting. It was also noted that NHS Digital will present the findings from an audit which has been looking at the information available on GP Practice websites about how patient data is held and shared. It was suggested that this topic could be shared with Healthwatch to understand how much knowledge the public has around GPs communicating their patient data sharing. The Communications and Stakeholder Engagement Manager will discuss with this Rebecca Moore from Healthwatch.
2.	**Formal noting of previous meeting's action notes** The action notes from the 10 November 2022 meeting were agreed and approved for publication.
3.	**Showcase of NHS Digital's Secure Data Environment (SDE)** The Delivery Lead for the SDE platform (previously known as a Trusted Research Environment -TRE) gave a presentation about NHS Digital's Secure Data Environment, followed by a pre-recorded demonstration of the SDE by the Product Manager. The following key points were made: - All users of an SDE require a Data Sharing Agreement (DSA), a legal document, to be in place which follows a process, of which the

	Independent Group for Accessing Patient Data IGARD is an element, to ensure only those organisations with an acceptable purpose, and approval against set criteria, have access. - The individual SDE users must be part of an organisation that has a DSA in place with the NHS to access the SDE. - The login process for the SDE is via two-factor authentication (using a password and code sent to a mobile phone) - like the security used to access personal online banking. - The SDE provides access to a secure virtual desktop that is hosted inside the secure environment. This desktop has access to pseudonymised data that cannot be removed without it being subject to some form processing that generates a dataset that is aggregated and anonymous, and is subject to approval by trained NHSD staff. - The SDE uses cloud computing to provide power for processing. - The data is "minimised" in accordance with the DSA so approval is only given to access the least amount of data necessary to fulfil the purposes. Only approved, pseudonymised data can be accessed and in a secure way. - Data in the SDE is pseudonymised with a unique key for each user per DSA, meaning that data in one dataset cannot be compared against data in a different dataset within the SDE. - Only anonymous aggregate data that has been approved by trained output checkers (individuals) may be removed from the SDE. - An SDE allows researchers to collaborate on the code they are writing to analyse data. - Linking to other datasets provisioned via the SDE are made linkable by default and it is possible to link to data that is brought into the environment assuming it contains the required information. - There are strict governance processes around the SDE and there is a manual review of SDE activity to ensure legitimate and safe access. - There is a multi-layered approach to security, designed to provide a series of safeguards, significantly reducing the risk of data being compromised. - The SDE has an audit capability that logs who ran what query, at which point in time, against what dataset to give transparency around what users have been doing with data. The panel raised the following questions about the SDE which were responded to by the Delivery Lead: - ***Could researchers, for example, be able to link anonymous data that can be taken out of the SDE?*** Data can only be linked within the SDE. Only aggregate, anonymous, data with no identifiers can be taken out of the SDE and only if it is approved by the governance process. Data taken out of the SDE that is anonymised cannot be linked to any other data. Therefore, researchers for example will have to use the SDE, but they can bring their data to the SDE to link to data sets held in the SDE. - ***Would the Secure Data Environment be where GP data would end up once the programme is delivered?*** Yes, it is one of the commitments to only allow access to GP data via the SDE.

Action notes

	- ***How is the cloud computing part secured?*** The virtual compute is contained in the private NHS cloud. This is not accessible to anyone other than the NHS (including staff of suppliers who support delivery of the platform). The NHS owns the servers used to host the cloud, all data is encrypted and only the NHS hold the keys.
	
	- ***Who provides the cloud services?***
	  - AWS from Amazon provide the cloud computing infrastructure and services that the SDE platform is built on. The data stored in Amazon is encrypted and the keys are owned by the NHS. Amazon cannot access the data, it is fully encrypted. NHS simply buy infrastructure from Amazon and is provided advice by Amazon about how to best use the technology.
	  - Databricks is also procured as an analytic package (Software as a Service - SaaS) that is hosted on AWS that the NHS buys. The staff from Databricks are unable to access the data held in the SDE, however the NHS analysts and users are able to access the data using Databricks.
	  - Immuta provide software to control data access.
	  - Development of this platform has been completed by developers from Accenture who have ensured all working on the SDE have or are in the process of applying for SC clearance while the build is being completed for security purposes
	
	While software and infrastructure are provided by commercial providers, they do not have access to the data in the SD .
	
	- ***Is there an audit trail?*** – Yes, Immuta controls access and it logs who has accessed what and how, showing the queries that each user has run. The intention is to move towards active monitoring, but how far that gets will be subject to funding and stakeholder priorities once the SDE is operational. An example of how the audit trail works in practice was shown in the demonstration.
	
	- ***What are the principles of who can access the SDE – does it align with the the 5 safes model)?*** Yes, ONS has defined the 5 safes (projects, people, processes, settings, and environments) to ensure that data within SDEs is kept safe. Only users under a DSA are able to access the SDE. There is a planned SDE accreditation that NHS want to launch to ensure that the research has been accredited, so it can be “approved” and certified that research done in an SDE is correct that will align with the 5 safes model. All users of the SDE will be trained and approved to use the SDE.
	
	- ***It was noted that data from GP records and hospital records as well as other data sources that can be linked securely; this was well received. It was questioned if this is the mechanism that individual patients can use to access their data?*** No, this is not for citizen access as the public would not be able to get a DSA, however there are other programmes concerned with increasing citizen access to their patient information.

Action notes

	- ***Are there safeguards in place to stop abuse of the SDE by NHS data scientists?*** There are end user agreements for any individual accessing the SDE which cover the appropriate use of data including terms of operation in the environment. The Communications and Stakeholder Engagement Manager took an action to seek further information on this to feedback to the Panel. - ***What are the plans of communication around the SDE to the public? Perhaps an animation or video would be useful?*** There is a communications and engagement workstream. It was agreed that they be invited to a future PPECAP meeting and an offer of support from the PPECAP made to support the work. This will be actioned by the Communications and Stakeholder Engagement Manager. Further to the discussion, the Panel felt it would be helpful to understand the end-to-end process of the customer journey, from making a data access request through to accessing the SDE. This will be added to the agenda for a future meeting. It was commented that previously data was being transmitted to organisations in possession of an approved DSA with responsibility being placed on them for appropriate handling and disposal of the data, so moving to an SDE is much better and this improvement needs to be communicated to the public. It was suggested that a diagrammatic version of the infrastructure layers, which sit around the SDE, be produced to support the public to understand the security and offer reassurance. The Communications and Stakeholder Engagement Manager will raise this with the team leading the SDE communications and offer the support of the panel to review and advise on the communications. The Panel felt reassured that SDE users' actions would be logged and that data cannot be copied out of the environment. They welcomed the news that 'keys' in different environments means that data cannot be copied and shared which they felt was important. Overall, the Panel felt significantly more reassured having learnt more about the SDE, the controls in place to keep data secure and that only a limited number of authorised individuals would have access to the data. They express a need for it to be well communicated to the public and there was a strong feeling that this should cover explaining previous data sharing arrangements to demonstrate how much more robust the new model is. The Panel members thanked the SDE team for their presentation and for taking their questions.
4.	**In person meeting discussion** A survey, undertaken with Panel members revealed there was a desire to meet in person, but that hybrid arrangements would also need to be in place. A date will be pencilled in for the new year and a meeting invite circulated as a placeholder.

Action notes

	The majority of respondents identified London as being the most convenient location in the survey, however there was suggestion to explore venues in Birmingham. This will be looked into and further views sought. The preferred timing emerged as 11am – 3pm, to support travel arrangements. It was agreed that all the rotating useMYdata representatives would be welcome to attend. The frequency of face-to-face meetings was discussed, whist the value of meeting in person was recognised, there was a strong feeling they should be no more than twice per year. A panel member asked if a senior leader could be invited to attend for part of the meeting. This suggestion was welcomed by other panel members and the request will be made.
5.	**AOB** It was conformed that the scope of the PPECAP has been broadened to cover the direct care work, as per discussions in previous meetings. Topics for the next session - Web content to support the ambient campaign. Pre-work to be circulated for panel members to inform the discussion. - Findings from the GP Practice website audit. - Future topics: - How data is used for research uses - SDE communications - NDG presentation linked to GP Data – commercial arrangements & data flows beyond the NHS - Presentation on the governance arrangements supporting access to the SDE No further points were raised.

ENDS