Regulatory Sandbox Final Report: NHS Digital

A summary of NHS Digital's participation in the ICO's Regulatory Sandbox Beta

Date: December 2020

Information Commissioner's Office

Contents

1. Introduction

1.1 The ICO introduced the Sandbox service to support organisations who are developing products and/or services that use personal data in innovative and safe ways and where such products and/or services deliver a potential public benefit.

1.2 In order to develop the Sandbox, the ICO initially launched the Sandbox as a beta phase, for an initial group of participant organisations during 2019 – 2020.

1.3 The beta phase provided a free, professional, fully functioning service for ten organisations, of varying types and sizes, across a number of sectors.

1.4 Organisations who were selected for participation in the Sandbox beta phase have had the opportunity to engage with us; draw upon our expertise and receive our advice on mitigating risks and implementing 'data protection by design' into their product or service, whilst ensuring that appropriate protections and safeguards are in place. NHS Digital was one of the candidates who was selected for participation in the Sandbox beta phase.

1.5 During their involvement in the Sandbox, NHS Digital began to explore the development of a central consent mechanism through which individuals could expressly agree to share their health data for purposes beyond their care and treatment, such as research. The plan centred around three use cases, one of which was a 'permission to be contacted consent model'.

1.6 A scoping meeting was held between representatives from NHS Digital and the ICO Sandbox team in Leeds on 12 August 2019, and a further plan development meeting on 4 December 2019. Following on from this, objectives for NHS Digital's Sandbox participation were agreed and the Sandbox plan was approved and signed off on 14 January 2020. NHS Digital progressed with the plan until late February when work had to be paused as a result of the need to re-deploy its internal project team resources to support the NHS response to the coronavirus pandemic.

1.7 As the coronavirus pandemic progressed, in June 2020, the Sandbox engagement was re-scoped, to focus upon supporting NHS Digital in its development of a central mechanism through which individuals could sign up to be contacted by the researchers working on the COVID-19 vaccine studies. In July 2020, NHS Digital launched the COVID-19 Vaccine Studies Permission to Contact Service ('PtC') or the COVID-19 Vaccine Registry as it is also sometimes referred to publicly, in partnership with the National Institute of Health Research (NIHR), the research partner of the NHS in England. This first of its type UK-wide NHS-developed online service allows members of the public to register their details to give their permission to be contacted by researchers working on the NIHR approved UK coronavirus vaccine about participating in their studies.

1.8 This reports outlines the work that the ICO Sandbox team supported NHS Digital on during its time in the Sandbox Beta, particularly since June 2020 in relation to the PtC service.

2. Executive summary

2.1 NHS Digital's original Sandbox plan objectives were agreed in January 2020 and some preliminary work was carried out around the following, with support from the Sandbox team:

- to understand the challenges in obtaining and managing patient consent for use of their data in the health and care sector for purposes beyond their individual care and treatment;
- to map out some different data flows through the central consent mechanism to understand what items will be required in the user journey and for additional data processing activities such as data sharing; and
- to identify and assess the risks inherent in the consent mechanism processing and to implement appropriate technical and organisational measures to ensure the protection and integrity of patient data.

2.2 The Sandbox plan was re-scoped in June 2020, to focus specifically on supporting NHS Digital with the development of the COVID-19 Vaccine Trials Permission to Contact Service ('PtC'). The preliminary concept work that had been carried out

under the above objectives, including understanding around risk identification and mitigation, consent and lawful bases under Article 6 of the GDPR in a healthcare context, added value to the re-scoped work.

2.3 The ICO Sandbox was included as one of the key stakeholders that NHS Digital requested support from whilst developing the PtC user journey, and drafting of the data protection impact assessment (DPIA) and the user privacy notice.

2.4 The key data protection considerations that were discussed during the engagement included:

- ensuring transparency around the processing, including in relation to the interplay between the GDPR requirements and the legal framework surrounding patient data, such as the obligations of confidentiality and consent under the common law duty of confidence;
- reflecting on the proportionality of the proposed method of processing;
- assessing the risks to data subjects posed by the PtC service; and
- implementing reasonable measures to mitigate the risks identified.

2.5 Within the limited time available, the ICO was able to provide feedback on the privacy notice and the online prototype user journey, before the service was launched to the public in July 2020. Although the DPIA did not meet the threshold under Article 36(1) of the GDPR for it to be submitted for ICO prior consultation, input on this was also provided to NHS Digital.

3. Product description

3.1 NHS Digital is the national information and technology partner to the health and care system in England. It was established under the Health and Social Care Act 2012 with statutory powers to collect, analyse and disseminate patient data under legal directions and requests, and to operate and provide IT systems on behalf of the Secretary of State for Health and Social Care and NHS England.

3.2 NHS Digital was commissioned by the National Institute of Health Research (NIHR) to provide the PtC service for the Vaccine Task Force via the nhs.uk website. NHS Digital has been directed by the Secretary of State for Health and Social Care under section 254 of the 2012 Act and the COVID-19 Public Health Directions 2020 (the COVID-19 Directions) to collect, process and analyse information for COVID-19 purposes. NHS Digital has also been requested under section 255 of the 2012 Act by the devolved nations in Scotland, Northern Ireland and Wales to collect, process and analyse information about residents in the devolved nations under separate section 255 requests for COVID-19 purposes. These statutory rights form the lawful basis providing a basis in law for the processing of PtC data in the exercise of official authority for the purposes of Article 6(1)(e) of the GDPR.

3.3 The PtC service consists of a front end website hosted within the nhs.uk website. The website allows members of the public to register an interest in being involved in COVID-19 vaccine research. Specifically, individuals are provided with information about the COVID-19 vaccine studies and links to NIHR's 'Be Part of Research' webpages, which provide practical information about being involved in the research. Individuals are asked for their email address and are then sent a link to verify their email before they are taken through some health related questions. This function is designed to make the service as accessible as possible whilst also reducing the risk of members of the public signing other individuals up using their email address without their permission.

3.4 Individuals are taken through a series of questions which NHS Digital, working in conjunction with NIHR and vaccine researchers, considered necessary for the service, which include health related and other relevant questions, for example, about what kind of occupation they have. The answers provided help to ensure that any information shared with researchers running a vaccine study is limited to people who are potentially eligible to take part. The volunteer is then asked for their permission for NHS Digital to share their email address and other relevant details with researchers whose studies they appear to be eligible for based on the questions asked in the user journey. The information provided to participants makes it clear that the individual is only giving their permission for researchers to make contact with them where they are potentially eligible to take part in a study and does not constitute the individual's consent to take part in a vaccine study. Such separate consent is obtained directly by the research body running the vaccine study after making initial contact with the individual, assuming the participant still wishes to continue with the vaccine study.

3.5 Within the user journey, a broader permissions statement was also included to give individuals the option to allow NHS Digital to contact them about the progress of the vaccine research and about updates to the PtC service in the future.

3.6 The PtC service is integrated with NHS Digital's Data Access Request Service (DARS) which reviews and approves applications by bodies running NIHR approved vaccine studies for access to data. Specifically, under a Data Sharing Agreement with DARS, bodies who are NIHR approved providers of COVID-19 vaccine studies are able to access the electronically captured information from the members of the public who have given their permission for researchers to contact them directly. The information provided by those who have signed up is accessible to researchers where the information provided by the individual matches the eligibility criteria for that particular vaccine study. Researchers, who are separate controllers, are responsible for contacting volunteers directly and for authenticating and seeking further consents from individuals to take part in their vaccine studies as per the usual clinical trial recruitment processes.

3.7 At the time the PtC service was launched, there were two NIHR approved COVID-19 vaccine studies being run by two institutions, Oxford University and Imperial College London. Since then, the Oxford study has been approved by NHS Digital to contact volunteers on the Vaccine Registry and a further NIHR approved study, the Novavax study, has also been approved to contact Vaccine Registry volunteers. It is expected that additional COVID-19 vaccine studies approved by NIHR and NHS Digital will be added over time. Those studies who are recruiting volunteers into their study using the Vaccine Registry are published on the NIHR website.

3.8 NHS Digital is the controller in respect of the data collected and used for the PtC service. Although NHS Digital is established in England only, the PtC service has been expanded out to allow individuals across the UK to register for the studies through the requests made to NHS Digital under s255 the 2012 Act. Joint controller relationships have been formed between NHS Digital and the Secretary of State, and also between NHS Digital and each of the devolved nation health bodies to determine the overarching purposes of collection, analysis and dissemination of respective citizens' data collected through the PtC service.

3.9 Some of the aims of the PtC service are:

- to support the aims of the Vaccine Taskforce, to drive forward, expedite and co-ordinate efforts to research and produce a coronavirus vaccine;
- to drive a footfall of 500,000 individuals to the PtC service by the end of 2020;
- to widen the opportunity for members of the public from across the UK to get involved in research to develop a COVID-19 vaccine, whilst having more control over how their data is used;
- to allow researchers to identify and recruit suitable cohorts quickly to the vaccine studies, reducing recruitment time and accelerating the delivery of an effective vaccine to manage the outbreak;
- to reduce the burden on front line NHS staff to identify and contact potential vaccine study participants; and
- to allow geographic and equality monitoring of volunteers to enable the PtC service to be developed in a way that will support the needs of under-represented groups.

3.10 There is currently no linkage between the information captured from individuals via the PtC service, and existing medical records held by NHS Digital. An individual's PtC registration will override any existing National Data Opt-out they have already registered for these specific purposes only.

3.11 It is expected that the PtC service infrastructure will be developed in the future to allow individuals to sign up for other research and clinical trials.

4. Key data protection considerations

Lawful basis and the common law duty of confidence

4.1 The sharing of the health data for purposes beyond the individual care and treatment of patients (secondary uses) such as research is considered a complex area and one which often causes debate within the healthcare sector. This may be partly due to the abundance of legislation and statutory/sector specific guidance that needs to be adhered to when processing confidential patient information, and the common law principles which apply to information which is subject to a common law duty of confidence. For example, the term 'consent' is used across both data protection legislation and the common law duty of confidence, both relevant in healthcare, and although intertwined, have different meanings and implications under the two laws. For instance, the requirements for gaining valid consent under the GDPR are different to those needed for collecting consent under the common law duty of confidence. Each also offers varying rights to the individual under their respective laws. This may cause confusion to the member of the public to whom the data belongs, in terms of which legislation their consent applies to and what their rights are.

4.2 In the context of the PtC service, an individual must give their consent under the common law duty of confidence for NHS Digital to share their confidential information, gathered through the health questions within the user journey, with the applicable researchers for which vaccine studies the individual appears to be eligible for. In addition to gathering individuals' consent in this respect, NHS Digital also required a lawful basis under Article 6 of the GDPR to carry out the PtC processing.

4.3 NHS Digital have been directed by the Secretary of State for Health and Social Care under the Health and Social Care Act 2012 and the COVID-19 Direction 2020 to collect, process and analyse information for COVID-19 purposes. This forms the lawful basis under Article 6 of the GDPR, pursuant which the PtC service was developed and used to capture data from members of the public. There was some discussion within the Sandbox engagement about whether this would constitute processing under Article 6(1)(c), 'processing is necessary for compliance with a legal obligation to which the controller is subject'. The ICO advised that although NHS Digital was under an obligation to operate the service through which the data

could be collected, processed, analysed and disseminated, for the purposes of the GDPR the processing of each individual's personal data was intended to be optional and was not therefore directly necessary for compliance with that legal obligation. Further, reliance on the legal obligation basis set out in Article 6(1)(c) would deprive individuals of the right to object, which would be incompatible with the nature of the PtC service and the right to withdraw from the service at any time. Reliance on the legal obligation basis in Article 6(1)(c) would therefore misrepresent the optional nature of the processing. It was agreed that the basis in Article 6(1)(e) 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' would be a more appropriate basis for the processing.

Transparency

4.4 Under Article 13 of the GDPR, controllers must comply with the 'Right to be informed'. This right is about providing individuals with clear and concise information about what you intend to do with their personal data. In the development of the prototype user journey, NHS Digital aimed to ensure that the information presented throughout was understandable and that it was clear to individuals what they are signing up for through the PtC service. NHS Digital asked the ICO Sandbox as a stakeholder for feedback on the 'consent' wording within the user journey, and on the privacy notice to ensure that they were able to achieve this aim.

4.5 The ICO recognises that providing sufficient information to allow individuals to appraise the service and make an informed decision about whether to share their data, whilst also ensuring that there is not too much information included so that the reader is overwhelmed, can be a difficult balance to achieve.

4.6 Specific feedback was provided by the ICO, in terms of some of the language used to describe the processing within the user journey, which resulted in amendments being made to the privacy notice, to ensure clarity was provided around NHS Digital's role in the PtC service.

4.7 Through the ICO's engagement with NHS Digital, it was understood that there is a chance that an individual who has not completed the PtC user journey and did not provide their permission for NHS Digital to share their data with researchers,

could be contacted to participate in COVID-19 vaccine studies without their permission, where the law allows. Although data gathered through the PtC service will not be linked to other existing health records about the same individual already held by NHS Digital, an individual may be contacted to take part in similar research via other means. For example, in England, the law permits data to be requested through applicable laws such as section 251 of the NHS Act 2006 and the Health Service (Control of Patient Information) Regulations 2002 (COPI), where the research has been approved by the Secretary of State or the Health Research Authority. This would be coincidental and would not be a result of the individual using the PtC service. The possibility of this occurring was not made sufficiently clear within the privacy notice, and additional wording was added to reflect this and increase the transparency of these other processes. As s251 and COPI is not applicable in every devolved nation, wording and external links to information affecting individuals who live in other areas of the UK was also included.

Necessity and proportionality of processing

4.8 NHS Digital requested feedback from the ICO Sandbox on the Data Protection Impact Assessment associated with the PtC service. Specifically, the ICO considered that additional information should be added to the DPIA to ensure clarity around the necessity and proportionality of the PtC service. These important elements of the GDPR, include an assessment of the method of processing and whether it could be achieved by less invasive means and with less personal data, in accordance with the 'data minimisation' principle, Article 5(1)(c). The amount of data that is collected and the method used should be balanced against the benefits of the intended processing. The benefits of developing a COVID-19 vaccine and driving a sufficient footfall of participants to vaccine testing are clearly demonstrable and in the public interest. The ICO suggested some amendments to the DPIA to reflect this, including describing the benefits of the proposed method. NHS Digital included additional detail of the benefits in relation to the different stakeholder groups (NHS Digital, frontline NHS staff, individuals signing up, members of the public and researchers).

4.9 A broader permissions statement at the end of the user journey was included in the PtC service, asking individuals for their permission for NHS Digital to contact them about other research in the future and to inform them about updates to the PtC service. It was agreed between the ICO and NHS Digital that this statement, as originally drafted, was not specific enough

and did not provide individuals with sufficient information about what they were giving their permission for. Further detail was added to the statement within the user journey to provide further clarity around what this contact would entail, and additional detail was also included in the privacy notice. We understand that NHS Digital has since reviewed this aspect of the service and split this statement into two permissions to provide individuals with more specific choice and control over their data in respect of such processing.

Risks to individuals

4.10 NHS Digital and the ICO discussed a number of data protection related risks that may be posed by the PtC service and how these could be reduced or mitigated to an acceptable level.

4.11 Due to the tight time restrictions that NHS Digital were working within prior to launching the service, the development of an authentication functionality to verify users was not considered to be practically feasible. This meant there was a risk of a member of the public signing up another individual to the service without their knowledge or authorisation. NHS Digital therefore established at the outset that the PtC service could not obtain a permission to link the PtC service data to health records, and that all data required by the vaccine studies would need to be provided directly by members of the public through the sign up process. To mitigate against the risk of an individual being signed up with their email address without their knowledge, NHS Digital implemented an email confirmation process within the user journey. This means an individual would need to provide their email address and then verify this through a confirmation link sent to their email, prior to continuing through the user journey and giving their permission for their data provided through the PtC service to be used. This email confirmation was considered a reasonable control to mitigate the risk, whilst the linkage of the PtC service data with other health records is not part of the service.

4.12 Another risk discussed was about the potential for individuals to fall victim to phishing scams. This is because they would be expecting email correspondence from the researchers connected with the vaccine studies. This risk is heightened due to the number of bad actors seeking to take advantage of individuals during the pandemic and the increase in online scams. NHS Digital suggested that telling the individuals what the official email addresses would be that they could expect to receive

genuine communication from, could help to mitigate the risk of individuals responding to phishing scams from other contacts. However, the ICO considered that the potential of the official email addresses being spoofed (a bad actor imitating a genuine email address) was still possible. Therefore additional information was added to the privacy notice to caution users of the potential for scams and external links to resources such as Action Fraud and the National Cyber Security Centre that could provide further advice and support to individuals.

4.13 At the time of the PtC service launch in July 2020 there were two NIHR approved COVID-19 vaccine studies being run by two institutions, Oxford University and Imperial College London. There is, however, the capacity for the number of studies to increase to around twelve, within the life time of the service. There was therefore a concern about individuals being contacted too many times by either the same researcher or multiple researchers and finding this email contact intrusive. To limit the risk of this, NHS Digital imposed a limit on the number of times a researcher can contact an individual within a given period. As well as this, individuals have the right to withdraw their permission to be contacted as a result of signing up to the PtC service, using the original email address they signed up with. This functionality is also available on the nhs.uk PtC service landing page. Although this would not delete the data from NHS Digital's systems, researchers would no longer be able to contact the individuals who had withdrawn their permission from the service.

4.14 It is not possible for an individual to participate in more than one vaccine study. NHS Digital implemented a feedback loop requiring researchers to provide information back to NHS Digital when an individual was successfully recruited into a vaccine study. Information pertaining to that individual would not then be shared with other studies and the participant would not then receive unnecessary contact from researchers.

4.15 NHS Digital and the ICO discussed the eight year retention of PtC data, following the last use of the data obtained through the PtC service, including an individual's withdrawal of their permission to be contacted. This retention was set in accordance with NHS Digital's records management policy to enable NHS Digital to audit the data use and to exercise legal rights and respond to any potential legal claims that may arise from the processing. The ICO provided feedback regarding the risks of keeping data for extended periods, for example, the information becoming inaccurate.

5. Ending statement

5.1 NHS Digital's participation in the Sandbox has allowed the ICO to gain additional insight and build on our existing understanding of the sharing of patient data for secondary uses such as research in the health sector, including the interplay between data protection legislation, the common law duty of confidence and other applicable laws and statutory guidance. This knowledge will be shared internally within the ICO and is hoped to support colleagues engaging with stakeholders in the health sector.

5.2 The Sandbox was of great assistance to NHS Digital during the development of the PtC service. The service was developed under incredibly tight timescales and NHS Digital has fed back to the ICO how the Sandbox team were engaged and responsive, contributing valuable subject matter expertise throughout. Respecting privacy, upholding data subject rights and maintaining public trust were at the heart of NHS Digital's and NIHR's vision for the PtC service. Participating in the Sandbox gave NHS Digital and NIHR confidence that they had achieved these aims at the point of launching the service and has enabled NHS Digital to consider future developments to the service in line with these principles.

5.3 The ICO understand the benefits to all of society in developing a safe COVID-19 vaccine, and the PtC service is clearly an important part of this. At the time of writing this report, c.310,000 members of the public have registered using the PtC service. A public dashboard shows the number of volunteers in the UK and by local authority which is also broken down by age and gender. The Sandbox has found it a valuable experience to support NHS Digital and NIHR in considering compliance with data protection legislation and ensuring that individuals' are appropriately informed and their data protection rights are upheld.

5.4 The Sandbox recommend NHS Digital keep the PtC service and associated documentation under review and re-consider and address risks posed to individuals where the PtC service iterates with additional functionality.