On citizens controlling access to their health and social care data for direct care

A summary of the results of a research project at Teesside University.

We are grateful to the Information Commissioner's Office (ICO) for funding this project through their Research Grants Programme and for advice regarding rights and obligations under the GDPR when processing personal data.

All views expressed regarding the Privacy Preferences Tool are the responsibility of the author.

Jim Longstaff
j.j.longstaff@tees.ac.uk

2 October 2019

Contents

Abstract

A prototype Privacy Preferences software tool for citizens' health and social care data was developed and evaluated with focus groups comprising a wide range of users. The primary purpose of the focus groups was to evaluate the acceptability and ease-of-use of the software tool for sharing data for direct care. Fictitious data, based on real scenarios, was used in the evaluations. A possible use for a future commercial development of the tool might be in a Health Information Exchange system supporting access to records held in provider systems. The outcomes of the evaluation were that younger adults with significant computing experience could understand and use the tool, but people with less computer experience and confidence needed support. One conclusion was that the tool is appropriate for the citizen/patient to explore their data and to prototype sharing preferences; however, the preferences should only be turned into permissions which actually control access to data by a care professional during a consultation. This is suggested by several potential problems, including: adverse effects to treatment and care; difficulties with authentication; and, on the part of the citizen/patient user, lack of medical knowledge, lack of capacity (maybe unrecognised), insufficient experience with computing devices, and deliberate misuse.

1 Data Controllers and Processors

There is a need for anyone intending to make use of a Privacy Preferences Tool to identify data controllers and processors. The ICO has provided the following information regarding this topic.

Under the GDPR, one of the key challenges in the planning stages of sharing personal data is to identify the flow/s of the data, and at each point in the process determine who the controller/s and or processor/s are. This will enable better risk identification and mitigation and clarity of who will have responsibility and accountability at each stage and is likely to be unique depending upon the organisations and processes involved. Information about this can be found in the ICO's guidance on controllers and processors: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

If those looking to use the tool involve data from several sources, they may need to consider a distinction between controllers working together as joint controllers or alone as individual controllers. Joint controllers will decide between them on the purpose and manner for which personal data is collected; it will not be decided by one single organisation. There is more detailed information on this at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/

In terms of privacy information, data protection legislation also requires controllers and joint controllers to be transparent about their respective responsibilities ensuring that individuals know who to contact when they want to

exercise their information rights under the legislation. Information about the joint arrangements would need to be made to individuals and, irrespective of the joint arrangement, an individual may exercise their rights in respect of and against each controller.

Furthermore, it is also good practice to conduct a Data Protection Impact Assessment (DPIA) for any major project which requires the processing of special category personal data likely to result in a high risk to individuals. A DPIA should describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. ICO guidance on this process can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

2 Rights regarding sharing data

The GDPR requires practices to process data 'fairly' and in a 'transparent manner' which is 'easily accessible and easy to understand'.

Therefore the information provided to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. There is more detailed information on this at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

In order to process personal data securely compliance is required with two laws: Common Law duty of confidentiality, and Statutory Law (GDPR, DPA 2018).

Using the Privacy Preferences Tool will include the processing of special category data and the GDPR provides this type of data with more protection. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. This is because this type of data could create significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Organisations will need to show you have considered this when detailing the lawful basis for your processing. Further information on this can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/. Implied consent is the mechanism for Common Law compliance within the Tool, although it must be noted that while consent for sharing may be withheld under Common Law, the basis for processing data under GDPR may mean that information is nonetheless appropriately shared between organisations and care professionals.

Provision for opting out of sharing data via a Local Care Record or Health Information Exchange system should be available.

Citizens have the right to restrict the sharing of their health and social care data, except in certain cases where legal requirements apply such as involvement of third parties, notification of communicable diseases, etc. Guidance on GDPR and privacy notices offered by the BMA is available at: https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr/gdpr-and-practice-privacy-notices-ppns

However restricting availability may have severe consequences. In extreme situations, the General Medical Council Ethical Guidance for Doctors, para 31 advises that ongoing treatment might be suspended where the patient refuses to share data deemed essential. https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality

As well as a right to restrict access to data. under the GDPR individuals also have the following rights regarding their information:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

In certain cases where legal requirements apply and form the lawful basis for processing, some of the above rights will not apply. For example, when processing on the basis of legal obligation, the individual has no right to erasure, right to data portability, or right to object. Further information can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

3 On sharing computerised care records

The five missions of NHSX, the team which is to drive digital transformation for health and social care, are:

- To reduce burden on staff, so they can focus on patients
- Provide citizens with tools to access information and services directly
- Clinical information can be safely and digitally accessed
- Improvement of patient safety across the NHS
- Increased NHS productivity

(as expressed at the Digital Healthcare Show, London, June 2019 by the NHSX CCIO).

Additionally, it has been stated that setting privacy preferences should be part of the NHS App, and not be carried out by an application built on top of it.
See https://healthtech.blog.gov.uk/2019/05/31/the-nhs-app-a-platform-for-innovation/

Furthermore, the Local Health and Care Record Exemplar (LHCRE) projects have the functionality of preferential sharing of data for direct care, and patients contributing information about treatment progress.
https://healthtech.blog.gov.uk/2019/06/24/nhsx-giving-patients-and-staff-the-technology-they-need/

An objective of at least one major Health information Exchange project (HIE) is that fine grained authorisation should be required, to the level of a patient telling a GP that “this information is only for you”.
https://www.greatnorthcarerecord.org.uk/information-for-care-professionals/principles/

4 Citizens views on sharing data for direct care

A substantial public engagement study has been carried out for the Great North Care Record project. The results can be found in https://www.greatnorthcarerecord.org.uk/wp-content/uploads/2018/09/GNCR-public-engagement-report-FINAL.pdf.

Some findings which are relevant to our Privacy Preferences Tool project were:

- Citizens generally trust the NHS to manage their data, but have less trust in commercial organisations or the police. Commercial and for-profit organisations are the least trusted.
- Most people are happy for their data to be shared for their care. However they wanted granular control over e.g. restricting sensitive or stigmatising data to those who needed to know.
- Citizens said they would like to have access to data held about them, both to see what is said about them and to add additional information like organ donor preferences.
- They expected to be given control over their decisions about information sharing and did not think that health care professionals should make decisions on behalf of patients or citizens.
- Across the focus groups citizens struggled to describe what they would like a sign-up process and registering their consent to look like due to the lack of a visual or interactive model to engage with.

Many other studies and opinion polls have addressed this topic. The PRSB held a “Twitter chat” in May 2019: one view expressed by a contributor was that he didn’t want care professionals (henceforward abbreviated CPs) who he interacted with to know about a particular problem which was not relevant to the treatment or support they were providing.

5 Supporting the sharing of data

Henceforward we use the term ‘citizen’ to generally include ‘patient’. Taking into account citizens’ wishes as expressed in focus groups, and the requirements for lawful processing, we propose the following approach for setting sharing controls:

- Permissions controlling access to data generated at a healthcare institution to be set by a Care Professional (CP), according to legal requirements for processing carried out at that institution (e.g. at a GP surgery). Therefore, the CP is ultimately in charge for processing data, taking the citizens’ directives into account.
- The citizen has the right to direct the CP to deny access to selected data for the purpose of direct care. However, this is not possible when there is a legal requirement for sharing.
- If the citizen wishes to deny the sharing of data under Common Law which the CP deems essential for direct care, the citizen can be offered the following option. The CP can make the data available to CPs working at other institutions who need to access it (i.e. to teams, roles, or team/role combinations), while denying it to others. An indication of the existence of concealed sensitive data will be given to all CP users, who would have the option of choosing to view sensitive restricted data, if they judged it necessary. Messages can be displayed to CP users advising situations when the sensitive data should be accessed.
- When legally required appropriate access will be provided to the appropriate authorities.

6 Privacy Preferences Tool

6.1 Procedure for developing preferences and permissions

The overall approach can be summarised as follows:

1. A citizen-user executes queries on their data, and explores the results,
2. Preferences are defined,
3. Preferences are verified by executing further queries and observing the alterations in the retrieved data,
4. Preferences can be further reviewed by inspecting simple natural language statements of their meaning,
5. Unwanted preferences can be deleted.
6. Preferences can be turned into permissions which actually control access to data during a consultation with a CP.

Preferences can be prototyped and developed either during a consultation with a CP who receives and enters them, or by citizens themselves if they have been provided with an online account.

Extensive help and guidance buttons and links appear on all screens.

Citizen-users are advised that an indication of sensitive data withheld in the first instance will be displayed to a CP user, who will be able to access this data if they are advised to, or exceptionally if they think they need to. All accesses are recorded and audited and can be inspected by the citizen-user.

Citizens have the option to contribute information about their care, and to set preferences on the information they contribute.

6.2 Authorisation functionality

Extensive authorisation functionality is provided by the Privacy Preferences Tool, as follows:

1. Preferences can be specified for pre-defined summary concepts such as a health condition, situation or circumstance. Our experiments worked with a simple master-detail presentation of problems/situations associated with detailed record entries. More detailed presentations could have been used, e.g. the MIG presentation. https://healthcaregateway.co.uk/services/detailed-care-record/ or a subset of the PRSB Core Record https://theprsb.org/wp-content/uploads/2019/04/Persons-core-information-standard-010419-aggregated-v2.html. However the same preference-setting and searching capabilities are achievable with the simpler presentation.
2. Preferences can be specified for individual record entries, such as issuing a prescription, or noting an opinion gained from a telephone consultation. These entries are expressed as free-text, and can be linked to one or more summary concepts indicated in 6.2.1 above, if appropriate.
3. Preferences can be expressed and implemented at both general levels of detail (e.g. my health data can be shared with any CP who is treating me), and at fine grain levels (e.g. my psychosis data can only be shared with my current GP, the specialists who created it, and a Psychiatrist I am referred to).
4. Preferences can be defined for hierarchically structured teams (where a team consists of other teams and CP users), and CP roles (also hierarchically structured). For example, certain data might be seen by a team leader, but denied to other members of the team.
5. Preferences can be defined for team/role combinations. For example, data could be generally withheld from team members, but made available to a sub-team (or specific individuals in the team) associated with a certain role.
6. Break Glass authorisation functionality is provided to optionally define progressively stricter levels of access to sensitive data, with selectively defined overrides for teams and roles.

6.3 User Roles

1. Citizen. This role includes the patient and social service client roles.
2. Care Professional. This includes healthcare professional roles such as GPs, allied health professionals, doctors, and social service care professionals.
3. Healthcare Administrator. An administrator role for care-related matters and users.
4. System Administrator.

6.4 Usage Modes for Creating Preferences

6.4.1 Standard Mode

This mode provides limited functionality for preference prototyping and is suitable for citizens/patients.

1. It supports specification of constraints on sharing summary data, as defined above. A list of the citizen's main problems (a summary list) is displayed, and an item selected.
2. Then a list of commonly recognised CP roles is displayed, and the opportunity afforded to deny access to CPs in one of these roles. Other roles can also be explored and selected.

6.4.2 Advanced Mode

This mode provides additional authorisation functionality over Standard Mode. It could be used by a CP developing and demonstrating preferences and permissions to a citizen, or by citizens prototyping preferences themselves. Its functionality includes:

- Denying/permitting summary data to selected CP roles.
- Denying/permitting record-level data to selected CP roles.
- In particular "Display sensitive data" controls can be defined, to display data which the citizen would prefer to be concealed on a first access. Their effects can be demonstrated to the patient.

6.4.3 Healthcare Administrator Mode

For Healthcare Administrator role only. Its functionality includes:

- Standard and Advanced Mode.
- Privileged access – creating more powerful preferences giving access to sensitive data than can be created using Advanced Mode.

6.5 User Role Functionality

6.5.1 Citizen

- Standard and Advanced Mode Preference Development – the user can select between these modes.
- Querying at both 'normal' and 'display sensitive data' access levels.
- Contribute information relevant to their care.
- Review preferences and permissions.
- Delete unwanted preferences.

6.5.2 Care Professional

- Standard and Advanced Mode Preference Development – self-selected.
- Query at both ‘normal’ and ‘display sensitive data’ access.
- Review preferences and permissions.
- Delete preferences and permissions as directed by patients.
- Specify messages to be displayed to other care professionals.

6.5.3 Healthcare Administrator

- Includes Care Professional role functionality.
- Development of preferences/permissions at Healthcare Administrator Mode.
- Querying at privileged access level.
- Creating, managing and overseeing patient and CP accounts

6.5.4 Systems Administrator

- Includes creating and provisioning Healthcare Administrator accounts, and provisioning the Care Professional and Citizen roles.

7 Focus Group Evaluation

7.1 Method

The sessions took place in a Teesside University computing laboratory, where the Privacy Preferences Tool was separately installed on the laboratory computers. The focus group sessions started with a group introduction to the tool followed by a demonstration using fictitious data based on a real scenario. Participants were then given an opportunity to familiarise themselves with the tool on a lab computer and execute a query using the scenario. Subsequently a group discussion was then followed by another session using the tool, to set preferences unaided for a different scenario. This was followed by a final group discussion. Participants were discreetly observed and supported individually at times while testing the tool.

7.2 Summary of results.

1. The ability to specify individuals for open access and restrict it to others was appreciated. Participants thought that it would be useful to specify which data was restricted too.
2. There was concern that the public would not understand the tool’s purpose, the social data that was covered and the individual roles of practitioners. In particular, they anticipated that certain groups, possibly those who are especially vulnerable such as the elderly and those with learning difficulties, would struggle to understand the purpose of the tool and how to use it.
3. Users with high levels of computing skills and experience (students and University staff) said that they found the tool straightforward, but all other groups found it moderate or hard to use in the time available. All participants managed to set preferences and restrict access with support. Less experienced and usually middle-aged or elderly participants said that if they were on their own computer,

were given plenty of time to familiarise themselves, could practice and write down the various steps required, then they would be able to use the tool independently.

4. All participants made suggestions to alter the terminology to increase usability. Many terms were said to be in ‘computer-speak’, used differently in common parlance and/or not words in current usage. Suggested amendments to terms were gradually being introduced during the data collection process to improve clarity.
5. Participants questioned if the level of knowledge among the general population, about medical conditions and health and social care systems, which was assumed by the tool, was realistic.
6. Support, it was suggested, could come in various guises, including increasing user-friendliness through design, online sources and personal mechanisms. For example: a video tutorial, improved navigational prompts, a Frequently Asked Questions sheet and/or step-by-step instructions. Specific groups, without the relevant computer skills, would definitely require personal support.
7. Data-sharing with care professionals was not a focus of the questions asked of participants; however, they expressed many opinions about it. There was broad agreement that it should be made available to medical staff but much more restricted for social care staff.
8. The idea that specific professionals could be given access was welcomed by some participants. Although it was recognised that there was a danger that patients/clients might not fully realise the impact of any restrictions to access.
9. That there was a choice other than everyone or no-one sees their data was well received. The potential this offered for their medical and/or social carers to work more closely together was viewed positively, citing opportunities to reduce silo-thinking and medical mistakes.
10. It was pointed out by participants that social care professionals require medical information also, to care well for their client e.g. about any long-term health conditions. Participants thought that, with the increasing use of care services for the elderly, this was likely to become a focus of the tool.
11. Boundaries to data access, where they should be drawn and by whom, was a major topic of discussion in Focus Groups 2 & 4. It was argued that the appropriate decision-maker was dependent on the situation. The list of decision-makers included:
    - Patient/client only
    - General Practitioner
    - Acute medical or surgical doctor
    - Allied Health Professional
    - Social care team lead
    - Care home manager
    - Carer.
12. Doctors were seen as experts, who might require wide access on which to base their medical/surgical decisions. It was suggested in one group that surgeons

should automatically have unrestricted access. While social care professionals were not spoken of as experts and the information they might require was expressed in vague terms and, it was suggested, should be decided on a case-by-case basis.

13. Confidentiality was seen by participants as a thorny issue when support was required to a) use the tool and b) to make personal data-sharing decisions. In their view, patients/clients could be open to having their opinions overruled, unless a system was provided to protect them. To limit this possibility as far as possible, participants suggested that patients/clients would benefit from the process being simplified.
14. The override for health and social care professionals, offered by the tool, spurred much debate among participants. They were acutely aware of the dangers of restricting data, especially to medical workers, although they liked the concept of choice; however, they were uncomfortable with the idea that their choice could be overridden. They favoured the view that the decision must be made in consultation with care professionals but accepted this was not always feasible e.g. if a patient was not in a condition to give informed consent, such as following an accident. Hence the need for an emergency button or override.
15. Most group members were in favour of a mobile version of the tool and thought it would appeal to the public, especially the young. However, some older people said they would be unlikely to use a mobile for this type of work. The feasibility of adapting it in an acceptable way was questioned, although there was support for an app if it could be done.

To summarise:

16. The tool was acceptable as a useful asset for accessing patient/client records. The requirement for a thorough, initial explanation of the purpose of the tool and how to use it was crucial to successful user engagement.
17. A high standard (degree level) of computer literacy was needed to confidently use and navigate this tool. Members of the public, with individual, personal support were able to execute queries and set preferences. The main barriers to usability related to terminology, presentation and navigation.
18. Participants were attracted to the idea behind the tool, to share data more effectively and usefully, through systems that complied with ethical governance processes to protect patients and clients. However, there were reservations about the robustness and feasibility of systems in restricting access.

8 Conclusions – the use of a Privacy Preferences Tool

The focus group studies did not directly address some wider issues of data sharing:

- Authentication of citizen/patient users. How can it be guaranteed that a user restricting the availability of medical data, which might be crucial to their own treatment and safety, and maybe that of others, is who they say they are. There is always the possibility of coercion by other family members or acquaintances.
- Deliberate misuse. Where a user might restrict data for purposes other than the benefit of their care and well-being. An example might be a patient addicted to prescription drugs visiting several healthcare providers to obtain them.

For these and the other reasons outlined above, we suggest it is not appropriate to allow citizens to set permissions which control access to their health and social care data independently. However, a Privacy Preferences Tool could be used for citizens to explore their own data and develop preferences which could subsequently be turned into permissions in a professional care environment, following advice from care professionals. Citizens would still be in control over who could access their data (in so far as they are legally allowed), but the problems of potential lack of understanding, inadequate computer skills, authentication, and deliberate misuse could be minimised or eliminated altogether.