Understanding health data security in direct care: co-creating information and resources with the public

April 2025

Authors and project team

Kohlrabi team

Dr Fran Harkness- Project Lead

Dr Adebisi Adeyeye – Qualitative lead

Facilitation, design, and additional analysis:

Katie Tiley

Aisha Ofori

Yaning Wu

Ngozi Nwybonyi

Understanding Patient Data team

Emma Morgan – Research & Evidence Manager

The team thank the members of the public for giving their time and sharing their invaluable views with the research team, the expert stakeholders for their thoughtful insights, and the project Steering Group for their helpful guidance and advice on the project throughout the process.

Executive summary

When people use health services, information is added to their patient record to support their safe and effective care. Research has shown that many people are positive about providing their data for direct care purposes and their record being shared between staff and health services (1) (2). There is recognition that giving staff the information they need makes care more safe and effective and avoids patients having to repeat themselves.

However, in general the public have long been concerned about security threats to their personal data (3), and there is little public awareness or understanding of what is done to specifically keep health data safe within direct care settings (4). Several recent pieces of research from the Patients Association have reported that patients want honesty about how their health data is kept safe due to concerns about leaks or misuse, including transparency about whether NHS systems are good enough to prevent this (1) (5).

The Information Commissioner's Office (ICO), the UK-wide independent body which offers information, guidance and enforcement in data security, describes personal data breaches broadly as a security incident affecting its confidentiality, integrity or availability (6). If the public is to feel confident that their health data is kept safe, research first needs to understand what security and 'breaches' of their data mean to the public, and secondly, how to make the systems and people behind data security visible.

Understanding Patient Data (UPD) commissioned this research to work with the public to understand perceptions and knowledge of health data security and explore solutions to information gaps identified in the desk review. A sequence of public involvement activities between January and March 2025 began with a deliberative dialogue of 47 members of the public exploring what the public wants and needs to know about health data security in direct care settings, and how that information should be communicated. Building on the resulting insights, three smaller groups of the same public members (totalling 15 people) co-created specifications for public-facing explainers of health data security. These were then tested factually through six interviews with health data security experts and reviewed by the project Steering Group.

"This day has made me think about myself and my priorities. I was living free, not thinking about this. I've realised its personal information, vital to me. I should have more say." Dialogue participant

The findings derived through the deliberative dialogues and the co-creation process underpin the following four principles for producing and communicating public-facing health data security information. Each has implications for the development of a set of resources to be produced by Understanding Patient Data, to empower the public to better understand the basic facts of health data security and to make informed choices about their own data.

Principles

The following four principles were derived from the feedback from the public participants with the expectation that they will shape future communications in this area:

1 **Information should feel personal:** This research was a reminder of how little public knowledge there is about data security in general. Until participants viewed health data security concepts through the lens of their own lives and started asking questions, their knowledge gaps were filled by faith and assumptions. Relatable examples helped build understanding and sense of control. **Co-creation participants developed visual storylines for an animation and interactive infographics, with relatable characters to bring key health data security information to life. These storylines were refined through subsequent rounds of co-creation and expert interviews to ensure the events and wording were both accurate and resonant.**

2 **Transparency builds confidence:** Participants' realisation of their knowledge gaps raised feelings of low agency and anxiety, aroused suspicions that information was being hidden, and encouraged seeking answers from unofficial sources. Participants saw no reason for information not to be clearly and comprehensively communicated to them. Many people were pragmatic about data use and its security: risks in life exist and they and the protections in place should be visible. **Co-creation participants developed plain language narratives - acknowledging concern without creating fear, while clearly explaining rights and protections. Content and characterisation aimed to depict how data and breaches are handled in practice, while avoidance of dense text, jargon, and over-crowding of information improved the sense of transparency.**

3 **Proactive assurance of accountability and action**: Participants didn't just want facts about risks - they wanted improved knowledge and trust that the security safety net was there and that they would be alerted if and when there is a risk to them. **Specific wording was a challenge due to variation in roles, organisations, and processes across services, regions, and time. Co-creation participants humanised faceless organisations, and utilised serious tone and repetition to make evident a clear through-line of core principles across the system.**

4 **Useful information - now and into the future**: Participants had some concerns and questions which had not been anticipated by expert stakeholders. In addition, there was a strong desire for understanding of what a breach might mean for them and what practical steps they could take in response. However, while some queries may be answered easily, some are beyond the scope of one resource, and in some areas, the 'answers' are changing as society evolves. **In co-creation, participants shaped a layered resource: an introductory animation to build awareness, followed by flexible infographics which could be copied into printouts to start building people's understanding before something goes wrong. To be useful in the face of uncertainty, information was presented in the steps which people can expect in a data breach, and signposts were suggested to offer further support and information.**

Report Contents

1. Introduction

Sharing personal information with and between healthcare providers during care is a routine and expected aspect of modern health services. Research has shown that the majority of people feel positive about providing their data for direct care purposes and their record being shared between staff and services (1) (2), recognising that over time the rich information contained in health records helps to make care more safe and effective and avoids patients having to repeat themselves.

However, in general the public have long been concerned about security threats to their personal data (3), particularly as the information that people disclose to their health care providers may be especially personal. A recent NHS Digital survey revealed that 44% of a public sample (2,200 people) have information in their medical record that they wouldn't want anyone else to see, and around two thirds wouldn't want anyone who isn't directly treating them to have access to their medical records (7).

Despite these sensitivities research has shown that the public has very little idea how their health data is protected (4). While health data security concepts or issues are undoubtedly complex, several recent pieces of research from the Patients Association have reported that patients want honesty about how their health data is kept safe due to concerns about leaks or misuse, including transparency about whether NHS systems are good enough to prevent this (1) (5).

While the use and security of health data for secondary research has rightfully been considerably explored with the UK public (8) (9) (10) (11), the rapid systematic review stage of this project identified that there has been little work to capture what the UK public already know or would like to know about the security of their data in a direct care context (2). It was also identified that there is little or unclear existing public-facing information transparently communicating the risks and the safeguards in place to protect health data from breaches, defined as data being accidentally or intentionally lost, destroyed, accessed or disclosed without authorisation (12).

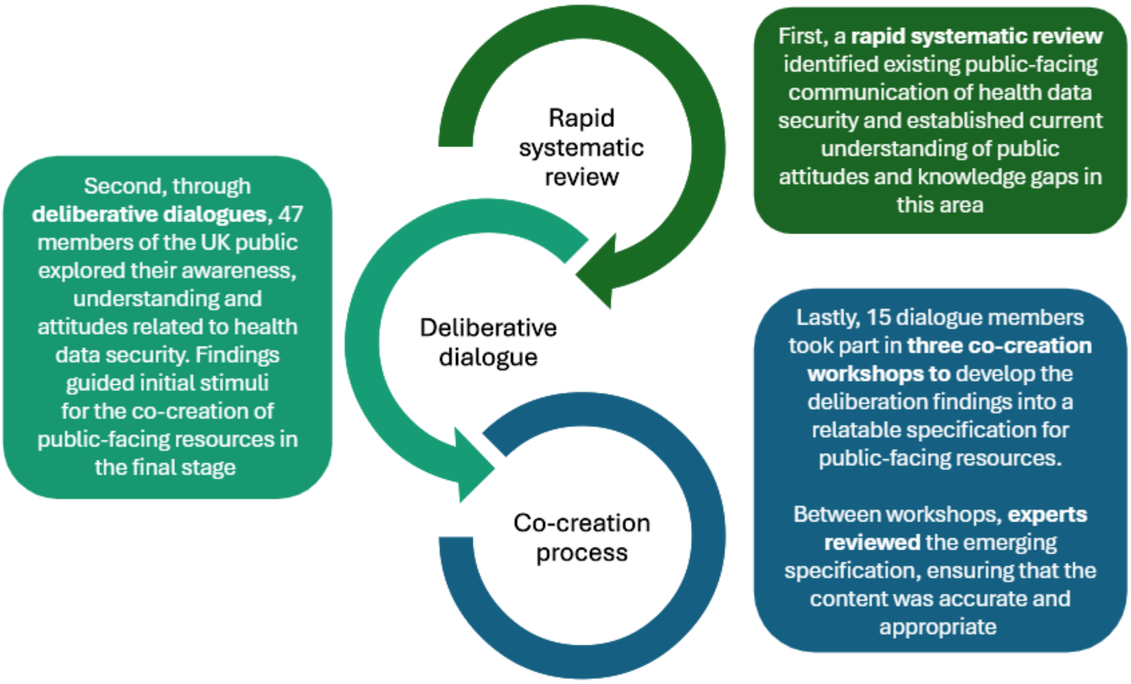
If the public is to feel confident that their health data is being kept safe, research first needs to identify what security and 'breaches' of their data mean to the public, and secondly, how to provide clear and meaningful answers about why and how patient data is protected in direct care. In this context, Understanding Patient Data commissioned an independent research team, Kohlrabi, to undertake research with the following objectives:

• Gain insight into the public's understanding of health data security, and concepts such as accidental breaches versus intentional misuse, cyber-attacks, and impact of data loss.

• Consider the public's feelings towards these topics, their information needs, and their perspective on how they would like information to be communicated.

- Co-develop specifications for public-facing resources based on the above, with the type, content, and design of resource being recommended by participants.

A three-stage methodology was designed to answer each objective, with each stage building on the previous insights. All fieldwork took place January 2025 and March 2025.



First, a **rapid systematic review** identified existing public-facing communication of health data security and established current understanding of public attitudes and knowledge gaps in this area

Second, through **deliberative dialogues**, 47 members of the UK public explored their awareness, understanding and attitudes related to health data security. Findings guided initial stimuli for the co-creation of public-facing resources in the final stage

Lastly, 15 dialogue members took part in **three co-creation workshops to** develop the deliberation findings into a relatable specification for public-facing resources.

Between workshops, **experts reviewed** the emerging specification, ensuring that the content was accurate and appropriate

Figure 1: Visualisation of the three stages of research

2. Project methodology

2.1 Design and accessibility:

Inclusivity and accessibility were at the core of research activities designed to produce outputs which engage a diverse UK population. Participants were supported to have their accessibility needs met, including the following considerations:

- Fieldwork was largely conducted remotely using an online video conferencing platform, improving inclusivity for those who would find it harder to attend in-person.

- One day of deliberative dialogues was conducted face-to-face in London to include participants with different learning styles, low digital confidence or exclusion.

- Most of the fieldwork was conducted during the week, however a weekend workshop supported inclusion of a wider variety of working patterns.

- For digital attendees, support was provided to hire laptops and book quiet spaces. The design was tested for suitability for joining via either mobile, tablet or laptop.

- The design included space for breaks to prevent fatigue or discomfort; with extra space tailored for those with caring responsibilities or needing prayer breaks.

- Attendees were thanked for their attendance with a £100 voucher for the deliberations and £50 for the co-creation workshop, reducing the cost of participation and in recognition of people's valuable time.

2.2 Recruitment

It is important that the information produced on this important subject meets the needs of the UK as a whole, not just the people of one area or background. In addition, the success of deliberative dialogues rests on people with wide-ranging perspectives learning not just from facts, but by considering the topic through each other's views and experiences (13).

With those principles in mind, a purposive recruitment framework was designed to recruit representatives from demographic categories of gender, ethnicity, age, socio-economic position, and residence across the four UK nations. Including a spectrum of health service usage was also important because people's experiences with the health system may shape how they understand and value their data. No other personal characteristics were collected, thus balancing the aim of representation of a variety of experiences with respect for the principle of data minimisation (14).

The design also considered how to include members of the public who would not typically be invited to or find involvement opportunities. The aim here was to reflect a fuller picture of public needs and concerns, especially of voices less frequently heard, but who may have high stakes when it comes to how health data is used and protected.

Primarily, recruitment was undertaken by twelve ‘community researchers’, i.e. trained lay members of the public, one living in city, suburban, or rural/coastal areas in each of the four nations, for example in Scotland this included Central Glasgow, a suburb of Aberdeen, and rural Pitlochry. Each community researcher produced and employed their region-specific recruitment strategy to reduce local barriers to engagement and participation.

Potential participants were either engaged with directly, via local networks, businesses and community services, or indirectly, via physical leafletting, posters, and online social media groups. Trusted community groups, such as language centres, sports and hobby groups, and advice centres, meeting the needs of the range of demographics listed in the purposive recruitment framework in each of the four nations also disseminated the opportunity through their physical and virtual networks.

2.3 Participants

A total of 50 participants registered for the initial workshops, with 47 attending. Participants were asked to confirm that they were over 18 and currently living in one of the four UK nations. For the co-creation workshops, a subset of 15 dialogue members were invited to participate. Participant demographics are presented in Appendix I.

2.4 Our approach

Deliberative dialogues

A deliberative dialogue approach was chosen for the initial stage of public involvement, as it enables informed views to be developed from a starting point of little prior knowledge of this complex landscape. Workshops were held in January and February 2025 across three identical sessions - one in-person and two online.

Typical to deliberation, differently situated members of the public were organised into small, facilitated groups (4-5 people), with plenty of time and space to discuss and learn from each other’s perspectives and experiences. During the five-hour workshops, trained deliberative facilitators from the Kohlrabi team followed an agenda and semi-structured topic guide to maintain consistency.

Each workshop began with an overview of aims and agenda, which participants had received in advance during onboarding. Aside from a brief explainer presentation from UPD introducing the current health data security landscape, the day was spent in guided group activities. These included discussing hypothetical case studies of different types of data breach, discussing perspectives on key concepts, and critiquing existing public-facing communication and media articles. The design encouraged peer discussion, reflection, and active co-learning, with facilitators supporting constructive dialogue throughout.

Co-creation workshops

The co-creation workshops held throughout March 2025 were designed to ensure that the final resource specification genuinely reflected public priorities around health data security. Building on the deliberative phase, three co-creation workshops were held, each comprising of five participants, drawn from the original sample (15 in total). To ensure a broader mix of perspectives, participants were selected to include at least three individuals from each nation and a diverse range of demographics - spanning gender, ethnicity, age, and experience of using health services.

Participants developed creative specifications for their preference of a short animation and four interactive infographics. Each three-hour session was structured using a topic guide to allow ample time for participants to contribute ideas and collaborate freely, guided by facilitators through a series of structured activities.

Across the three sessions, participants reviewed example materials, co-developed storylines, characters, visuals, and language, and iteratively shaped the tone, content, and structure of the proposed resources. The first workshop validated choices drawn from the dialogue findings, while the second and third sessions allowed participants to build on each other's ideas and integrate recommendations from expert interviews.

Expert Interviews

The final publicly resonant resource(s) and recommendations need to be factually accurate and aligned with health data protection industry standards. Therefore, between each co-creation workshop the emerging specification was reviewed through 30–60-minute semi-structured interviews with health data experts, cybersecurity professionals, and communication specialists in the field (for roles, see appendix II).

At least two interviews were intentionally scheduled to follow every co-creation workshop, allowing the researcher to address questions and clarifications that emerged during the workshops. This approach ensured that expert feedback directly informed the development and refinement of each resource. A general topic guide was developed and tailored to each expert's specific area of expertise.

Steering group

A project Steering Group was created to ensure key stakeholders were involved to advise and support on the direction and development of the research. People invited to be members of this group had relevant expertise across the health service, data protection, AI, cybersecurity and public involvement across the UK. Members are listed in the Acknowledgements section at the end of this report.

2.5 Analysis

All qualitative data was recorded and transcribed. Transcripts were inductively coded by a researcher, rather than matched to pre-determined categories. Findings could therefore emerge from the data rather than being imposed, as is important when working in areas where understanding is still forming. Two researchers identified key themes and subthemes, supported by quotes and contextual examples to ensure rich interpretation.

Preliminary analysis of the deliberative dialogues was validated with workshop facilitators and shared with the project Steering Group in advance of the co-creation phase. This allowed us to keep learning, using new insights to shape ongoing stages of engagement and clarify areas where we needed to ask more questions.

Drawing on participatory design principles, co-creation offered a second layer of interpretation, enabling participants to challenge and build upon findings. The dialogue findings were used by the research team and UPD to develop initial content and format options for the resource specifications. Co-creation participants directly developed these materials into specifications for health data security 'explainers', drawing on their own views and that of their peers from the dialogue. After each co-creation workshop and expert interview, transcripts were coded, themed and refinements were made to the creative and narrative direction of the emerging specifications.

The final four themes, which incorporate the dialogue, co-creation and expert interview findings, form guidance and insights for the current project, as well as for others working in the field to meaningfully communicate about health data security to the public.

2.6 Strengths and limitations of the methodology

The methodology offers key strengths that enhance the integrity and relevance of the findings. Deliberative dialogue is well-suited to build understanding of a complex topic for participants with little technical knowledge. To balance informed insight with instinctual reactions, workshops began with activities exploring participants' interpretations of terms like "health data" and "security". Participants said the workshop structure - logically building information through interactive activities, case studies, and reflections - supported their learning and allowed their questions to be answered.

The inclusive recruitment was a major strength, designed to capture a broad spectrum of views. Participants were purposively selected across different demographics, healthcare use patterns, and lived experience. Every online breakout group included at least one participant from each UK nation, supporting relevance across devolved nations. The involvement of community researchers in recruitment increased the likelihood of hearing from people not typically engaged in public involvement work.

Accessibility was prioritised, for example participants chose their preferred format and availability. While online research carries a risk of fatigue, regular interaction and breaks were used to maintain engagement, and evaluation feedback rated the online format highly for accessibility. Participants reported that the use of virtual whiteboards for instructions and note-taking improved their ability to follow discussions. Face-to-face workshops were offered for the co-creation process but participants preferred online.

The phased methodology - progressing from deliberation to co-creation and finally expert validation - meant that insights were iteratively refined and tested at each stage.

Facilitators and the project steering group validated themes before they were explored further in co-creation. Expert interviews, placed between co-creation workshops, helped verify accuracy and address technical gaps while keeping participants' priorities central.

Several limitations must be acknowledged. The sample was not intended to be statistically representative, and the relatively small size cannot reflect the diversity of UK public opinion. Although six data protection experts provided valuable technical input, they did not include perspectives from Wales or Northern Ireland. Despite our best efforts to make the information non-specific and standardised to allow it to cover all the nations, this may affect the perceived generalisability of the resources across the UK.

The length - one day for deliberation and three hours for each co-creation session - meant that while participants could develop informed views, there may not have been time to explore all aspects of such a complex topic. While a combination of group and individual activities, written and verbal input options, and careful facilitation prompted a wide range of perspectives to be captured, as with all qualitative work, there is a risk that some individual views may have gone unheard. Ultimately, these conversations can be seen as a starting point for continuing to involve the public in engagement about health data security in the field.

3. Findings

Interpretation of health data security information

While definitions of health data security exist in legislation and governance, the workshops made clear that for the public, their meaning is currently missing or different – being reconstructed through assumptions and personal experience. The expert conversations held during co-creation stressed the need to provide an improved public consciousness of data security in direct care: of what they can and should expect, with wording and tone which demonstrates that fears and concerns are taken seriously.

Introducing conversations about "health data" and the Information Commissioner's Office (ICO) definition of it were a reminder that it is easy for people not to realise how much information could be in patient records. Even those who were initially ambivalent became more engaged once they reflected on the possibility of a lifetime of names, addresses, symptoms, test results, appointment letters, and prescriptions - and imagined the potential consequences of its loss or misuse. Some only wanted security information to be readily available for answers in these scenarios, while some wanted to know how *their own* data was being kept secure in order to feel more in control.

Participants emphasised the need for clear, relatable explanations that reflect real-world concerns. There was unease about malicious external breaches, such as cyber-attackers, but the perpetrators and outcomes of these attacks were so unclear to most people that the threat felt distant. More distressing were everyday scenarios - such as staff who knew them in a personal capacity "reading" their data without authorisation, or neighbours or family receiving their patient letters. Practices considered routine by professionals, such as the use of older storage or communication systems such as fax or paper copies or legitimate data access by non-clinical staff, felt uncomfortably close to a breach for participants, or at least opened the door to error.

The insights from this public dialogue and co-creation process point to a mismatch between formal governance frameworks and public expectations, highlighting the importance of transparency and communication grounded in people's lived experience. Those communicating about health data security should not assume knowledge or shared understanding from the start but work with the public to humanise information and articulate what is important – both to the public and those working to keep data safe.

3.1 Expanded findings

The deliberation conversations illuminated four areas of consideration for any resource aiming to communicate health data security to the public. Findings are illustrated by anonymous quotes from dialogue participants.

1. Information should feel personal

The dialogue conversations underscored how personal the topic of health data is, yet how little people know about its security in direct care settings. Participants understood and were widely positive about the fact that health data was collected for their care, and most had some level of assumptions or knowledge about how personal data is protected in general. However, understanding of the reality of these concepts within direct care was surface level, with sentiment about public services and data use itself providing answers to their questions when facts were missing.

“I think it is quite secure. I've got family members who work for the NHS and they were saying that if you were to log in to see patients' files there'd be a catalogue.”
Dialogue participant

“I've listened… it's enlightened me, but I think there's something hidden still, and I will stick with that, because from the pandemic, and the way they handled us I've lost a lot of trust.”
Dialogue participant

‘You wouldn’t look into this information unless something happens to you. Then, I have questions, the information needs to get in on the front foot’
Dialogue participant

People who had worked in, or had close connections to, roles involving personal data - particularly in health, education, or justice - appeared to have a relatively positive impression of how health data security is managed, and faith that protective practices are followed. Typically, these participants reported that they had enough awareness of principles such as GDPR, or even tools such as “encryption” and “secure portals”, and had few questions. At the other end of the spectrum, participants with little professional experience of data governance, who reported existing low trust in public services, perceived that there is a lack of information publicly on this subject. They suspected that information may be being hidden from the public to protect authorities from complaint. While many occupations increasingly involve data protection in some form, this finding is a reminder that policymakers and decision-makers in this space may struggle to predict the information that people outside of those sectors want or need.

Between the more vocal ends of the spectrum, there was a larger middle group characterised by low awareness and low concern - and in some cases, openly low interest. They had low personal use of the health service, therefore had less concept of the sensitivity of health data. They had never given much thought to data security and imagined they would only ever try to learn more if their data was misused.

A topic as seemingly simple as what counts as ‘health data’ exposed the need for more proactive public-facing information. In one activity, participants listed types of information they thought qualified as health data. Many were surprised by the volume and sensitivity of this spectrum, such as contact details, mental health symptoms, and appointment records. The exercise prompted reflection and positivity on how timely, accurate data is necessary for clinical decision-making, but also how vulnerable it would make them if it was in the wrong hands. When participants began to consider health data security through the lens of their own lives, considering their own information and circumstances, even those who had previously felt neutral or confident started to pose questions and articulate concerns. As one participant noted, people may begin to withdraw when they suspect something is missing, as they did at this point of the dialogue, filling gaps with information from peers or unreliable sources.

> “I’d like to be more intentional and deliberate about health data security and how it affects me. If you know more it helps you, even in the way you hear information.” Dialogue participant

The understanding of health data security concepts which participants gained during the dialogue gave members of each group an increased sense of power. While not changing their impressions entirely, sceptical individuals reported more faith as they learnt about processes which they hadn’t been aware of (for example, staff training, data security legislation, reprimands and enforcement from a range of bodies). Meanwhile previously trusting or neutral participants realised that they had started with very little information and felt that they had been very naive. Regardless of their initial perception, several participants expressed a desire to learn more, and a wish to *feel* more in control of their own health data through knowledge of where it is and how it’s being looked after.

Recommendations for communicating health data security information:

- **Make it relatable:** Participants engaged most when the content felt resonant to their own lives. They believed that relatable information from people who looked and sounded like themselves experiencing the reality of data security practices would help the public engage and start to understand these concepts better.

> “I want real everyday examples. Data is just numbers, words. Give a visual representation of what it means. It’s my blood pressure reading. It’s real lives. Putting the words into flesh and meat.” Dialogue participant

- **Use visual tools to build understanding:** Participants found it easier to understand and evaluate information when they could visualise typical practices. Visual presentations of health data security information were popular, with suggestions for animations, images or simple clear infographics.

- **Layer information accessibly:** Many participants overestimated how much they knew before the sessions. It was thought sensible to start with the basics and allow people to choose when and how to explore further detail through the provision of layers of information and signposting to other trusted sources.

2. Transparency builds confidence

Participants' responded to the realisation of their limited knowledge of health data security with surprise, anxiety, and suspicion. Many felt frustration that public-facing information about health information security largely does not exist or is not as clear as it could be.

As health data security breaches in direct care were explored, many participants vocalised that it didn't make sense for organisations to attempt to shield the public from the potential for unauthorised access or loss of health data. Several participants had experienced incidents, such as receiving a family member's medical information. For others, their professional experience handling data helped them contextualise risk. They imagined that health services capture millions of patient interactions in data every day without much incident, and accepted that risks exist. Their ask was that these risks be articulated and explained openly, and that the associated protections, "warts and all", be clearly visible and understood.

> "No one wants to think that these things happen, its daunting, the harsh reality is it has happened, it probably is going on, I'd want to know it might happen."
> Dialogue participant

A small number of participants reacted anxiously to case studies introducing health data breaches. For them, the "not knowing" and associated lack of control were unsettling. Some really struggled to see why anyone would steal health data or how it might be used, and filled their uncertainty with worst-case scenarios. This heightened the suspicion that public institutions obscure information to avoid blame. For example, in an activity reviewing existing public-facing communication on health data security, a National Cyber Security infographic was perceived as concealing information due to its dense text, jargon, and crowded design. Regardless of their level of concern, participants wanted more comprehensive understanding of the realities of health data security, included aspects they had issue with.

> "It's not that it's better for people not to know. Actually maybe if the information was presented differently we could engage more. People may be upset later if they are not informed" Dialogue participant

One key information gap in a contentious area was the realisation that many staff, not just doctors and nurses, need access to data for direct care reasons. The rapid review stage (2) found that most news articles focus on malicious external breaches, but the dialogues showed far more preoccupation with the risk of familiar people reading personal information and "knowing about them". There was widespread poor understanding of why a range of staff require access to health data, and doubt that non clinical roles such as receptionists were subject to the same training or data security standards. These roles were expected to be more likely filled by 'local people', with associated fears of gossip or judgement. Lacking proactive assurance that non-clinical staff are held to the same professional standards, some participants felt that such access blurred the line between appropriate use and violation of data.

Another key area of concern which appeared to require more explanation was uncertainty about how information might be stored or communicated between staff. Prompted by a presentation including the ICO's '[data security incident trends' graph](), participants realised that information might travel via post, hand, fax, email, or verbally - not just through secure digital platforms as assumed. They were surprised that communication methods which they viewed as outdated and potentially less secure were still used. Prompted by the review of a media article describing [a hospital being penalised for staff using WhatsApp during Covid to share patient information](), questions about how staff communicate with each other when clinical settings aren't "joined up" were raised. Reflection on the need for timely staff communication left curiosity and suspicion of what modes are used instead. Participants wanted to understand what safe, standard practice looks like so they could spot when something wasn't right and take action.

> "Even email really threw me. It's so manual. You'd think there's a secure process like a secure platform to share patient information between themselves. I'm shocked actually. Now I'd like to know." Dialogue participant

Finally, participants were curious how often direct care data breaches occur. The ICO's '[data security incident trends'](): graph was deemed to have confusing terminology and frequencies. Based on participants' desire for reassurance, an early draft of the specification labelled health data security breaches as "relatively rare." This was seized by co-creation participants as feeling incorrect, with the assumption that it would be impossible to calculate, especially for 'low risk' breaches. Instead, their wording highlighted that unauthorised access is *possible*. The experts agreed that it was more accurate to shift from offering misleading estimates of frequency to a message of realism that 'sometimes things go wrong - and when they do, this is how they are handled'.

> "People share information all the time. It makes up conversation. It must be hard to put a number on how many breaches occur. Surely it happens every day." Dialogue participant

Recommendations for communicating health data security information:

- **Use plain language:** Dense text, acronyms, and unfamiliar organisational names made participants feel deterred or suspicious. Information should be presented in everyday language and short explanations instead of industry shorthand.

- **Be upfront:** Address common fears about unauthorised access and data misuse straight away. The public already have enough information about health data breaches to form questions; if those aren't answered proactively, information is sought from other sources.

- **Shift perceptions:** Participants had assumptions about what safe processes might look like; both in the roles and modes of communications. Storytelling could be used to normalise the necessary and authorised journey of data in direct care.

3. Proactive assurance of accountability and action

Participants emphasised that honest information about risks must be balanced by evidence that there is a safety-net of real trained professionals, organisational processes, and legal frameworks, bringing reassurance and transparency that data is being protected. For some there was such low awareness and trust in the system that they felt the need to be more active themselves to understand more and respond effectively.

> “The minute someone gives me information, they’re washing their hands. I don't want to know unless I know someone else is sorting it.” Dialogue participant

Many participants had little awareness of the seriousness with which data security is taken - of legislation, preventions such as training, or deterrents to misuse. Doubts that professionals treat data security seriously and effectively on their behalf led some to suggest taking a more active role themselves. Participants imagined receiving alerts when their health record was accessed, to monitor and determine whether that access was appropriate, and call for accountability. Others were content to delegate responsibility, if they could trust that someone accountable was taking care of it. What united everyone was a desire for clarity on what to do if unauthorised access or loss of health data occurs, who to contact, and how they’d be supported. This knowledge gap was identified in the rapid review stage (2), with few articles giving the public specific instructions of what to expect or what to do following the occurrence of a breach.

> “The ICO keep themselves quiet. They have good information though. They could better publicise that they’re here to help people.” Dialogue participant

The public desire to be reassured of the accountability of professional bodies responsible in direct care settings was underscored by the warmth with which this knowledge was received. Information on the role of the ICO was received positively. In later co-creation sessions, participants assigned visual signs of strength to the ICO and featured them repeatedly, indicating faith in their role. Participants were delighted to learn that professional bodies like the General Medical Council could take action against staff where appropriate. A surprising number of people did not realise that direct care staff would be trained to protect health data from unauthorised access or loss. There was still doubt on the consistency of cultural and organisational practices but there was an openness to their existence. Rising awareness of a ‘learning culture’ for errors and tangible repercussions for malicious breaches, such as job loss or prison sentences, strengthened participants’ perception of there being a safety net behind their health data.

Some participants felt uncertain that professionals perceived breaches as they did. This contributed to a lack of trust that incidents would be handled in a way that aligned with their expectations. A key issue was the gap between legal definitions of a breach and how individuals understood the personal impact of privacy loss. Many were uncomfortable with the idea that some breaches - particularly those involving inappropriate access by someone who could be known to them - might be classified as ‘low risk’ and never disclosed. While some participants wanted full notification of all breaches, others felt that, at a minimum, the threshold for disclosure should be well explained. Several suggested that the public should be involved in setting those thresholds.

> “I want to understand what’s supposed to happen, so I know when something’s gone wrong.” Dialogue participant

Both the desire to be assured that organisations responsible are taking data security seriously and the instinct to monitor it themselves remained into the co-creation process. Co-creation participants helped develop wording that broke information into small, digestible chunks, used plain language, and introduced characters to represent “faceless” organisations. This approach helped people see that data protection involves real individuals, trained professionals, and legal frameworks - bringing reassurance and transparency. The stories developed a sense of a safety-net: both visually and with repetition of key information, often in check-list form to highlight its consistency. One participant likened the need for repetition of simple, joined up messaging to buying apples from different supermarkets: they look the same, wherever you get them.

The experts consulted made some suggestions, noting that some public expectations like naming individuals responsible for data governance or providing hospital-specific hotlines aren’t always feasible. Names change, roles shift, and the key is to focus on frameworks, not individuals, as the thread running through personal data use. Experts also felt early drafts of the resource put too much emphasis on the ICO, inadvertently implying that responsibility lies only at the top. In reality, health services do handle their breaches before and after cascading them to the ICO, and most are doing the right thing.

Participants and experts alike stressed the importance of tone. Information should be honest about the risks, but not alarmist and not lay blame in one direction such as on healthcare staff. The final message should leave people reassured: things can go wrong, but there are systems, safeguards, and people working to make them right.

Recommendations for communicating health data security information:

- **Make accountability visible:** Participants wanted to know *who* is responsible. Relatable case studies and humanised characters were suggested to show that real people - not just faceless institutions - are actively keeping data safe.

> “If I've passed my data on to you, I want to trust you. I want faces behind who is accountable. I’m not going to pass my data otherwise.” Dialogue participant

- **The golden thread:** Expert stakeholders suggested that focusing on the structures around data security as a clear thread, was less confusing than naming multiple titles of those responsible and nuances between regions, Trusts and services.

4. Information which is useful now and into the future

The dialogue conversations underscored the low sense of control that people can have about their data and how more knowledge can increase agency. While some fears and questions may be answered easily, some are beyond the scope of one resource, and in some areas, the information or 'answers' are changing as risk, policy and technology themselves evolve. Therefore, the information provided needs to useful to people, taking their real questions and fears seriously - while being honest about what cannot yet be explained or where options are limited. Relatable explanations may start the conversation, while preparing people to build on that knowledge in the future.

> "It would be trustworthy having questions answered before you ask them. You don't want an explainer where you have to keep probing, and then what? It causes suspicion." Dialogue participant

Most participants instantly translated broad health data security concepts into questions of "what does a breach mean for me?". They wanted to be prepared in order to feel more agency in their personal data. However, there was the recognition that they are busy, that this is not their area of expertise, and that they therefore need enough information to help them understand "when to care". That is, when in their busy lives to take action to challenge poor security practice or to know how to respond to an identified breach. Common proposals were that the resource include simple checklists or step-by-step visuals outlining what might happen in the case of a breach and how a patient might be contacted. Some suggested that breach *impacts* on individual members of the public should be categorised (e.g. low, medium, high impact) in order that they easily know when they need to take action. While fears of gossip, identify theft, or blackmail were articulated, many felt unclear what the harms of a breach were. The categorisation process would involve spelling out how exactly each type of breach could affect them.

> "I just wanna feel that I know what to do if something happens". Dialogue participant

> "(to improve public information) I'd like something straight to the point. Tells you this is what's going on and this is how it affects you. You learn what they're doing, how they're preventing it. There's empathy, if you're the victim I think you'd feel less alone." Dialogue participant

In the later co-creation stage, experts noted that clarifying exactly how breaches cause harm can be difficult. Once data is accessed unlawfully, tracing its use and therefore the impact of the breach is challenging. Risk and responses to it also evolve. The main point is that the access is unauthorised. Experts instead recommended that resources spell out the existing ICO risk categories in plain terms, to explain how decisions regarding mitigation of a breach are made, with links to more detailed guidance. For their part, co-creation participants adapted storyboards to underscore the emotional impact of breaches, including re-telling a story from a victim's point of view to help viewers relate to the distress caused, and therefore to know "when to care". To improve knowledge of the steps to mitigate harm, the structure of storyboards was re-worked into a step-by-step format for breach-aftermath; for example, the health service assesses the situation, then report to the ICO, and so on.

Participants raised several fears and questions, mostly around access to health data, which revealed a need for information they can practically use - now and in the future. To answer their queries participants proposed creating relatable stories of how others had dealt with an issue and tips or steps for them to follow. Interestingly, some gaps, such as confusion about whether patients give their consent for data to be collected on them in direct care, could be seen as knowledge which should come well before information on health data security. There was also a near complete lack of awareness about whether patients can ask to read their own data and how they would do that, or, less frequently, concerns about whether family members can access their data. There were some concerns raised about anyone accessing their data outside of the direct care setting, which to them included third party contractors supplying hospitals, as well as non-public sector researchers.

Dialogue participants suggested that they would prefer a layered approach to communicating the many aspects of this complex topic: providing useful and essential details upfront in an animation with the option for people to make their own way through interactive infographics of case studies about different types of breaches. They felt that members of the public who want to know more technical specifics about the issues raised can follow links added to the visual resources, or read text summaries on reputable platforms. The experts corroborated how broad the field of health data is and suggested that UPD leverage several existing resources created by themselves or other organisations by linking and signposting them within these resources to avoid duplication of efforts and save on cost.

> You can click and zoom in on certain parts, maybe, and you can make it interactive in that way. I like that, because then I have more control. Because if it's linear, I have to sit from the beginning to the end. This isn't how to put together an IKEA table, if its something I just need to know the end result of, I don't need to watch the whole thing". Dialogue participant

Participants imagined different uses for the information, which will need to be addressed in the same set of resources. Some imagined turning to it only in the event of a problem; others wanted it available in waiting rooms to raise awareness proactively. There was support for multiple formats, with emphasis that not everyone is online or learns the same way. While animations and videos were appealing, others wanted printouts or interactive scenes they could explore at their own pace. Suggestion of the resources being shown in healthcare settings, whether on screens or with scenes cut-out as stand-alone posters or leaflets, reminded participants that these messages should be cascaded through the health service and staff should be trained to explain it to patients. It was felt that consistent messaging would improve trust as well as improving accessibility of the information.

Nearly all participants and expert stakeholders agreed that, to be useful, information should be clear and engaging. They recognised that information could feel complex and alienating, and recommended layered communication, such as an introductory animation with hyperlinks. Co-creation participants developed wording in plain English, and felt that easy read animation captions, and translations for the animation and the interactive infographics would be beneficial. Many participants articulated how much they had enjoyed being consulted during this research project and that the public should be involved and properly engaged with even further on this subject.

> "This day has made me think about myself and my priorities. I was living free, not thinking about this. I've realised it's personal information, vital to me. I should have more say." Dialogue participant

Recommendations for communicating health data security information:

- **Anticipate questions and signpost clearly:** Participants raised reasonable, predictable questions - some beyond the scope of any one resource (e.g., third-party contracts, their own data access). Rather than ignoring them, acknowledge these topics and signpost to support people in asking more from the system.

- **Be Honest About What Can't Be Explained:** There were a number of grey areas where answers did not seem possible - such as exactly what a hacker might do with health data. Participants suggested that proactively naming "the missing information" and pointing to reliable external sources would build trust.

- **Clear response steps:** Many participants worried they wouldn't recognise a breach or know how to respond. While the specifics vary, explaining how breaches are handled - and the list of steps individuals should expect - was thought to offer reassurance and restore some sense of control

4. Content and design considerations for the resource

The deliberation dialogues illuminated the four areas of consideration above for resources communicating health data security to the public. From these themes and dialogue findings describing priority content and format preferences, initial stimuli were produced for an introductory animation to health data security and four interactive infographics communicating different types of breaches. The content and design were then developed with co-creation participants and expert stakeholders.

4.1 Priority content

During the dialogue, public participants were introduced to information about health data, typical health data security practices, and types of breaches. Their questions and requests identified the following topics for future health data security resources:

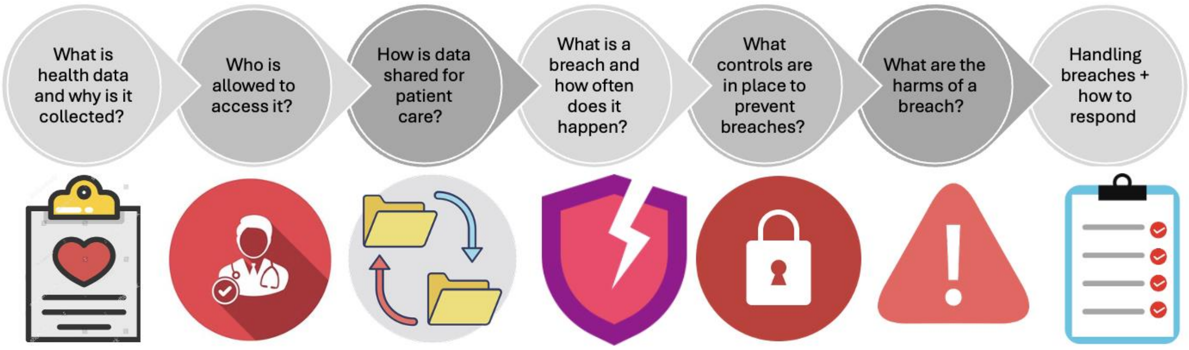

What is health data and why is it collected?
Who is allowed to access it?
How is data shared for patient care?
What is a breach and how often does it happen?
What controls are in place to prevent breaches?
What are the harms of a breach?
Handling breaches + how to respond

Figure 2: Visual depicting the seven categories of priority content

This section will take each of these topics in turn and outline why participants and experts consulted felt that this content was important, types of information they looked for, and the design implications for resources communicating these points.

What is health data and why is it collected

Participants realised that their interest in health data security increased when they thought about the amount and detail of information that may be stored for their direct care. Participants recognised the benefit of this information, i.e. "the risk" caused by authorised healthcare staff not having access to their medical history, for example. However, many agreed it's easy to forget just how much personal information the health service holds - until something brings it into focus.

> "I only started thinking about this in Covid when I got a vaccine text. I was thinking how do you know my name and number. I know they've got it but I didn't *know*".
> Dialogue participant

In response, co-creation participants re-wrote the first draft of the resource specifications to make the "life span" of patient information visible upfront, moving mention of it to the start of their explainers. They scripted relatable stories of realistic characters designed to remind viewers of the range of information about people's lives at stake: of names, addresses, sensitive diagnoses, appointments, and test results. They suggested several visuals where a volume of personal information is added to patient records. The stress in wording of “your care” and “your data” was developed to remind viewers of both the benefit and the potential risk of health data being used. Their aim was to trigger people’s journey of asking questions about data security issues. Experts consulted felt that the co-creation groups had built a good summary of what is meant by health information across different services and would only balance it with reassurance through wording such as “securely” or “restricted”.

Access: need and authorisation

Dialogue participants and expert interviewees agreed that the public needs a clearer understanding of who is authorised to access health data and why. Many participants assumed only ‘medics’ see their records - a perception which expert interviewees viewed as risky in its inaccuracy. In reality, a wide range of staff, including laboratory, radiology, and administrative teams, access data as part of delivering care. Receptionists in particular triggered surprise among participants, who had not realised how central their access to health data is to their role. There was noticeably less trust in non-clinical staff to uphold privacy and confidentiality, with some participants viewing them as "ordinary people"- part of the community - who might be more prone to gossip or judgement.

Initially the wording suggested for the introductory animation included the phrase “Only people directly involved in your care should access your patient record – this includes doctors, nurses and other clinicians.” The experts consulted urged that UPD utilises these resources as an opportunity to dispel this misconception. This would improve the public’s understanding on why broader access is necessary and how it contributes to better healthcare.

> "The phrase, ‘only people directly’ is tricky as there are lots of roles who also have legitimate access, like clinical coders, staff inputting test results. ‘Only people who need access as part of their job role’, would be more accurate.” Expert stakeholder

Although co-creation participants remained uncomfortable that non-clinical staff may “know about our lives”, they worked on phrasing and scenarios which expanded the ‘in group’ of authorised staff - based on role and need - and an ‘out group’ for anyone, including medics, who accesses data without authorisation. They wanted the public to be able to identify when there had been a breach and therefore when to take notice.

The flow of information for patient care: where does data go?

Participants expressed uncertainty about how their health data is stored and shared during care, with many assuming that it is always handled through secure portals or platforms, which would suggest authentication of identity and digital encryption. However, media reporting and ICO breach statistics explored during the dialogues revealed that a range of methods are still in use - including paper, verbal communication, and emails - prompting questions about what sharing practices are considered acceptable or safe. A media case study depicting hospital staff sharing information through WhatsApp during COVID triggered enthusiasm to learn what methods and platforms were now used for timely communication of health data.

> “I know very little about it. Are they making one big computer, or is it on the cloud. The data goes in, but where does it go?” Dialogue participant

Although participants were asking for explanation of what storage and sharing looks like, the expert interviewees verbalised that it is too complex to summarise the flow of information for direct care between staff and between health services. There is too much variation across settings, services, nations and situations. The important message is that no matter how the information is shared, its security should be guaranteed.

As with their feelings about data access, although the co-creation participants wanted the resources to spell out exactly how health information is communicated between staff, the bottom line was that the resources needed to have honesty about the potential breadth of methods. The case studies they co-developed included a variety of types of data sharing including verbal, email, and letters.

What is a breach and how often does it happen

Participants wanted clearer guidance on what counts as a health data breach - so they could feel confident that they could recognise it, to handle it themselves, or demand accountability. This desire to do their own monitoring reflects low underlying trust that those responsible for data protection were consistently upholding their duties.

Awareness and understanding of different types of breaches was low. Most time was spent talking about familiar scenarios - such as staff accidentally sharing information or accessing records out of curiosity - as they were imaginable. In contrast, cyberattacks felt abstract and distant. Participants struggled to imagine who might be behind external attacks, how they happened, or what stolen health data would be used for. They asked for information to make those types of breaches more concrete and relatable. Exploring existing information such as the ICO data security incident trends prompted more questions than answers: such as what does ‘other non cyber incident’ or ‘other cyber incident’ mean. The frequency of each type was also difficult to distinguish.

In the first round of co-creation, participants still struggled to bring to life the external malicious breaches visually, but focused on impacts such as the hospital not functioning as usual. Moving on to the frequency of breaches, they were keen not “to play it down”, eliminating initial wording from the materials such as “relatively rare”.

> “There's always a risk that anything can happen-- you can never stop a fire happening in your house, you can just minimise the damage.” Dialogue participant

There was a pragmatism that health data needs to be shared daily between patients and health professionals and between staff, and that the frequency of breaches would be hard to capture. The expert stakeholders consulted agreed that the information resource should shift from trying to give an estimation of risk, to imparting the sense that "sometimes things still happen".

What controls are in place

Participants wanted a clear picture of how health data is actually protected, underpinned by the need for reassurance that those responsible are taking health data security seriously. Unless their job gave them proximity to data protection, participants were either unaware or vague about measures health services might use to control against health data breaches. They wanted confirmation of the existence and level of staff training, confidentiality, security infrastructure, and deterrents such as potential fines and job loss. There was low awareness of the ICO, so learning that there was a body regulating and enforcing data protection laws was pleasing to people. People were generally positive about the NHS, but also doubtful of its efficacy in data security.

> "We're bombarded by press saying, 'the NHS is on its knees, they're rubbish'. You can imagine the training level has gone down. And I'm wondering how much they spend on security." Dialogue participant

In the co-creation process, participants developed ways to "spell out the safety net"; clearly breaking down the controls in place through checklist visuals, storytelling, avoiding jargon, and creating characters to give a face to legislators, the ICO, healthcare staff, and IT service providers. Making these bodies visible and relatable was thought to provide greater reassurance that these controls are in place.

> "We should add a character from the law or GDPR side. They say, "we do this, because of this, when this happens we do this". They need to be less mythical creatures." Co-creation participant

In terms of the narrative, the co-creation participants refined the starting stimuli away from chunks of information which gave the impression of information being hidden, and the inclusion of "a lot of big names without any breakdown", such as, 'Data Security & Protection Toolkit' and 'Data Protection Officer.' The expert interviewees agreed that it is more accurate to construct understanding of principles and frameworks as a consistent thread rather than titles or names which change over time or differ between countries.

Other wording additions from the expert stakeholders consulted included spelling out "multi-factor authentication" in a visual checklist of controls and reinforcing that staff training is "not just one-off training, it is or should be repeated at regular intervals, especially to stay up to date". Additionally, adding simple theory such as the reason why training is important was thought to enhance understanding and mental imagery.

> "You may like to add this is why regular training is important in the health sector so staff are more equipped to recognise how malicious cyber attacks can happen and what they can do to prevent falling for it." Expert stakeholder

Both participants and the experts consulted suggested signposting to further detail in the resources - such as the Data Security & Protection Toolkit, or advice on how to check if their GP surgery or hospital meets national standards - but only after the basics were made clear.

Lastly, for reassurance, several of the expert stakeholders highlighted how the language used in public communication can significantly influence the level of trust people place in institutions and their resources. They advised that these resources should avoid using overly cautious or qualified language such as "where possible," "however," or "we can”, as this can make messages appear uncertain or non-committal, potentially weakening public confidence in the guidance being provided.

> “(the first draft) is playing it too safe, it’s walking on eggshells, it’s potentially hiding something. It makes us think the topic is more serious than the text is giving.” Co-creation participant.

What are the harms of a breach

Participants longed to know exactly what someone does with their data once a breach has occurred - whether it’s a healthcare staff member accessing records without need, a member of the public accidentally receiving their appointment letter, or an external attacker breaking into a system. There was an emotional logic at play: if they could picture what the person was doing with their data - reading it out of curiosity, selling it, using it to target them or discriminate against them - they could better judge how much to worry about their health data security. This links back to wanting to be reassured.

> “How could we improve this information? I want to know the consequences of us losing track of our data.” Dialogue participant

Experts acknowledged that in many cases, it’s simply not possible to predict or trace exactly how misused data is handled. Instead of trying to explain the unknowable, some suggested focusing on clear explanations of risk categories - for example, cases where no one else saw the data and the harm is minimal, versus situations where access is unclear so harm must be assumed. Others emphasised that the core harm is the breach of legal and ethical duty itself: data protection laws exist for a reason, and when they’re broken, that in itself matters. This helps explain why even low-impact scenarios - like a member of the public receiving the wrong letter - are still breaches. Some participants also pointed out that the most significant harm may be when healthcare professionals don’t have access to the information they need to provide safe, effective care.

> “Some people are private but I’m relieved the NHS has this information. They need to offer the right care. If you’re unconscious, they need your history to help you.” Dialogue participant

Co-creation workshops built on these insights by shifting the tone of visual materials to focus on the perspective of those affected by breaches, conveying distress and vulnerability.

Handling breaches & how to respond

Participants wanted information on how services respond when a health data breach occurs - not in technical terms, but to provide confidence that appropriate action *is* taken. There was an uncertainty about how they, the public, should respond - driven by that lack of faith that someone else would alert them or handle issues on their behalf.

In early co-creation workshops, participants' minds jumped straight to repercussions, reflecting the gravity with which they wanted breaches to be treated. Initial imagery included "a data vault" being broken into by a burglar, who is caught, handcuffed, and brought before "an ICO judge" before going to jail. Red lights, sombre music, and visuals of large bags of money as fines represented the scale of wrongdoing.

However, expert interviewees noted that while the initial imagery was emotionally impactful, enforcement messages needed to be more realistic. Although the Information Commissioner's Office can make decisions, there is not an actual 'judge'. Additional enforcement characters were suggested both for accuracy and to "highlight that this is considered serious". For example, it might be appropriate to depict a police character next to the ICO. Other expert interviewees stressed the need to reinforce the central role of NHS seniors and professional bodies in managing breaches. They were keen for the NHS not to become demonised, suggesting scenes be moved around to show that the NHS would address breaches first.

In contrast to participants' initial imagery of punishment, experts recommended a softer tone: depicting a "just culture" in which organisations are supported by the ICO to learn from their mistakes. Through the ICO's guidance, shared lessons become part of the continuous cycle of improvement which staff and organisations can follow to prevent breaches. This may be a helpful visual for places where participants' ideas were limited by their knowledge, as may the idea of the ICO using a "regulatory toolkit" to improve practice and aid compliance.

Experts also pointed out that the original visuals lacked any sense of how a service might recover operationally following a breach. In response, co-creation participants suggested scenes showing calm returning: people in waiting rooms receiving texts with updates, queues going down, and x-ray machines restarting - representing services gradually coming back online.

> "There was a case study where data had been breached then they did this, this and this, and it turned out okay. That's useful. Like a story." Dialogue participant

4.2 Layers of information

Dialogue participants suggested that they would prefer a layered approach to communicating this complex topic: providing essential details upfront in an animation with the option to make their own way through interactive infographics of case studies about different types of breaches. They felt that members of the public who want to know more technical specifics about the issues raised can follow links added to the visual resources, or read text summaries on reputable platforms. The experts corroborated how broad the field of health data is and suggested that UPD leverage several existing resources created by themselves or other organisations by linking and signposting them within these resources to avoid duplication of efforts and save on cost.

Information on the following areas were requested as deeper layers of information:

Personal data agency: Although there was acceptance of the clinical benefit of data access and sharing, several participants had a sense that the 'implied consent' behind their data being stored and shared in direct care was not enough. They would have liked for it to be spelt out that the information they were telling their care provider may be used by other staff and retained for their care. The resources developed in this project aim to build more comprehensive understanding, but a simple explanation of implied consent may benefit some users. Additionally, low awareness of personal rights prompted suggestions for tips on how to access or redact their own records; guidance on access to health data for family members holding power of attorney; and information on how long health data is held for.

> "Are people given information on how your data is going to be used? I've never been told this. Do people know what they're signing up for when they're confiding in a doctor and giving this information?" Dialogue participant

> "There should not be automatic opt in. I want to feel like I have some control or power over my data" Dialogue participant

Direct care data for research: Participants felt that a line in the animation script describing "approved researchers" having data access raised too many questions for them. One expert observed that, in their experience, many people are not aware that their health data can also be used for research purposes, which can raise concerns around privacy and control. They stressed using subsequent layers of information to build understanding of how and why health data may be used for research, including information such as UPD's own webpages on the security of health data for research.

The role of third-party suppliers: Dialogue participants reacted with surprise and discomfort to a media case study about third-party contractors handling cybersecurity or health screening - expressing less faith in private contractors' ethical data protection, even while joking that they might have more expensive and therefore robust security systems. Experts consulted suggested that a subtle introduction to private entities in the animation could help avoid surprise. However, participants removed wording in the animation that, "all suppliers…comply with NHS standards", describing it as too abrupt.

They stressed that they did not want information to be hidden, but that this issue needed room to build their understanding before reassurance on security practices was possible. Following expert suggestion that this issue is likely an important topic in future discussions, signposting more information in the deeper 'layers' of text summaries would ensure the public is informed, before external narratives take hold.

> "I'm quite ignorant about NHS infrastructure. Do the private companies have it? Are they going to sell it? I don't want them looking at it." Dialogue participant

Access across services: Concerns also surfaced about health data being shared with other entities such as adoption services, employers, or the police, particularly among those with personal or community experience of being discriminated against by state systems. The concern was that information could be accessed by other public bodies when they were not expecting it and for a use that they were not satisfied with.

Organisational culture: In deeper layers of information, participants wanted more detailed information about the cultural practices around keeping health data secure. The human fallibility of security was very clear to them. For example, they wanted to understand the confidentiality principles in place - what they are, how they work, and the key content in staff training. Within this information, a glossary of key phrases like "confidentiality", "privacy", "data protection", "cyber incident," "non-cyber incident," and "phishing" was suggested to reinforce understanding and reassurance.

> "I don't know how the NHS values confidentiality and privacy as we're constantly told how bad the NHS is." Dialogue participant

Nuances: Participants from across the four nations of the UK were aware that the healthcare system can differ regionally, as well as across Trusts and services. Participants particularly wondered if and how data security practices vary across England, Scotland, Wales, and Northern Ireland. Acknowledging that synthesising and unpicking differences may be challenging, expert stakeholders suggested summarising elements that are consistent, and signposting to country- or setting-specific resources where the public could explore this further.

Risk in numbers: Some participants wanted to know the actual frequencies and statistics regarding the occurrence of different types of data breaches in the UK healthcare system. If existing statistics are hyperlinked in deeper layers of the resource, then additional information would be helpful; participants found jargon confusing and wanted plain English summaries of how to contextualise the numbers they were seeing.

Risk in terms of impact on lives: There was widespread dissatisfaction that the classification of breach risk - low, medium or high - had been set by the ICO and was interpreted by direct care staff, without inclusion of the public in the process. Participants wanted more examples of what low, medium or high risks would be, and to feel that their emotional distress even in 'low risk' scenarios was being respected.

4.3 The design

An initial set of stimuli was created from the deliberative findings by Understanding Patient Data, which co-creation participants developed into a final draft specification to support the resource production:

Storytelling device: Dialogue participants were united in desiring storytelling as a mechanism to bring health data security issues to life, with relatable issues and experiences exploring different scenarios plausible to them in direct care settings.

Visual format: The dialogue findings emphasised visual elements with a variety of formats for accessibility. Participants agreed on a headline animation, followed by interactive infographics, for people to make their own way through at their own pace. Participants spoke about being able to click through, zoom in and out, and being in control to find the parts they were interested in. Easy read text, language options, and plenty of space visually were suggested to enhance clarity and accessibility.

Relatable Character Representation: Participants explored using stick figures, to negate against any demographic feeling left out or stigmatised by the visuals, while real actors were considered to enhance emotional salience. Their middle ground was visual depictions of characters who were 2D but still realistic and clearly individual, for example differentiated by accessories and clothing, with expressive easy-to-read emotions.

Tone of gravity: Participants wanted the visuals to reflect the seriousness with which health data should be handled. Playful elements like animated bubbles or whimsical illustrations risked making the information feel trivial or amateur. To reinforce realism, participants placed stories in recognisable hospital settings, suggesting light backgrounds with contrasting characters - such as healthcare staff in blue scrubs and patients in bright clothing - to focus attention on the narrative.

Accountability/Depiction of official bodies: Participants were keen to feel assured by the responsibility of those with protection or enforcement responsibilities such as the government, the ICO, and healthcare services. Coupled with a vagueness as to the role of each, creative depictions included: a judge's gavel for the ICO; a computer screen locked in chains to represent cyber security; and a rogue character in black-and-white stripes being "put behind bars". Linking back to the ask for honesty, experts suggested more accurate depictions of officials while maintaining a serious, reassuring tone.

Sound: Reinforcing relatability, participants suggested narration with a mix of male and female voices with different British accents for variety. When probed about specific accents, most co-creation participants urged for "clear" and "easily understood" accents regardless of the region. There was little feeling about background music aside from neutral 'elevator-type' music, or one suggestion for thrilling music to trigger engagement. Upholding realism, there was consensus on natural noises to accompany the visuals, for example, a keyboard tapping, data 'whirring', or an email 'whooshing'.

Length: Several participants expressed concerns about the length of videos, specifying that anything over 3-4 minutes means it is hard to maintain their interest.

5. Summary and recommendations

This report, commissioned by Understanding Patient Data, responds to growing evidence that the UK public needs clearer, more accessible information about how health data in direct care settings is kept safe. To capture existing understanding and highlight information gaps, deliberative dialogues engaged 47 participants from across the four nations. Fifteen of these participants then collaborated to develop explainer resources, specifying content and delivery in a way that would suit and engage the public.

The main findings underpin the following four principles for producing and communicating public-facing health data security information, each with implications for the resource development:

1 **Information should feel personal:** This research was a reminder of how little public knowledge there is about data security in general. Until participants viewed health data security concepts through the lens of their own lives and started asking questions, their knowledge gaps were filled by faith and assumptions. Becoming informed through relatable examples helped participants feel more in control. **Co-creation participants developed visual storylines for an animation and interactive infographics, with realistic characters to bring key health data security information to life. These storylines were refined through subsequent rounds of co-creation and expert interviews to ensure scenarios and wording were accurate and resonant.**

2 **Transparency builds confidence:** Participants' realisation of their knowledge gaps raised feelings of low agency and anxiety, aroused suspicions that information was being hidden, and encouraged seeking answers from unofficial sources. Participants saw no reason for information not to be clearly and comprehensively communicated to them. Many people were pragmatic about data use and its security: risks in life exist and they and the protections in place should be visible. **Co-creation participants developed plain language narratives - acknowledging concern without creating fear, while clearly explaining rights and protections. Content and characterisation aimed to depict how data and breaches are handled in practice, while avoidance of dense text, jargon, and over-crowding of information improved the sense of transparency.**

3 **Proactive assurance of accountability**: Participants didn't just want facts about risks - they wanted improved knowledge and trust that the security safety net was there and that they would be alerted if and when there is a risk to them. **Specific wording was a challenge due to variation in roles, organisations, and processes across services, regions, and time. Co-creation participants humanised faceless organisations, and utilised serious tone and repetition to make evident a clear through-line of core principles across the system.**

4 **Useful information - now and into the future**: Participants had some concerns and questions which had not been anticipated by expert stakeholders. In addition, there was a strong desire for understanding of what a breach might mean for them

and what practical steps they could take in response. However, while some queries may be answered easily, some are beyond the scope of one resource, and in some areas, the ‘answers’ are changing as society evolves. **In co-creation, participants shaped a layered resource: an introductory animation to build awareness, followed by flexible infographics which could be copied into printouts to start building people’s understanding before something goes wrong. To be useful in the face of uncertainty, information was presented in the steps which people can expect in a data breach, and signposts were suggested to offer further support and information.**

6. Next steps

Participants suggested that, by addressing the concerns they had raised, effective health data security resources could be developed to improve public trust, awareness, and proactive engagement with data protection measures.

Understanding Patient Data will take this project forward by working with a creative design agency to further shape and develop the specifications and ultimately produce the recommended resources. As with all UPD's resource, these will eventually be available on a CC-BY license for all to use in their own suite of resources too.

UPD will also work to incorporate the recommendations shaped by this public engagement work into their broader policy messaging around health data security and beyond, ensuring that the public view continues to be heard and promoted.

Acknowledgements

Kohlrabi and UPD would like to acknowledge the commitment of the steering group participants in their advisory position during the entire project process, listed below. Please note, their contribution is not an endorsement of the outputs of this project. We also thank the respondents to the Call for Evidence.

Project steering group members

Phil Huggins, Director for Cyber Policy & National Chief Information Security Officer for Health & Care -Department of Health & Social Care
Rachel Clarke, Senior Policy Officer - Information Commissioner's Office
Dr Nicola Byrne/ Ryan Avison, National Data Guardian/ NDG Head of Office
Dr Alison Knight, Data and Privacy Specialist – Health Research Authority
Dr Frances Burns, Programme Lead - HSC Northern Ireland Trusted Research Environment, Co-Founder and Director– Northern Ireland Public Data Panel
Alex Newberry, Head of Research Involvement, Governance & Informatics - Health & Care Research Wales, Welsh Government
Mark Simpson, Policy Team Leader, Inclusion and Engagement - Digital Health & Care Scotland, Scottish Government
Dr Mahi Hardalupas, Senior Policy Advisor (Data) - The Royal Society
Dr Amir Mehrkar, NHS GP, Senior Clinical Researcher - University of Oxford, Director of Information Governance and External Relations - Bennett Institute for Applied Data Science
Pritesh Mistry, Fellow (Digital Technologies) - The King's Fund
Richard Ballerand, Executive Group Member - UseMyData

We would also like to acknowledge contributions from the remaining experts and stakeholders who chose to remain anonymous.

References

1. **The Patients Association.** Developing a data pact. The relationship between the public, their data, and the health and care system. [Online] 2023. https://www.patients-association.org.uk/Handlers/Download.ashx?IDMF=c348045e-4ffc-43e5-a2ce-8a21ca1c6c5e

2. **Kohlrabi, on behalf of Understanding Patient Data.** Health Data Security: Public Understanding, Perceptions, and Resources. [Online] February 2025

3. **Papoutsi, C., Reed, J., Marston, C., et al.** Patient and public views about the security and privacy of electronic health records (EHRs) in the UK: results from a mixed methods study. *BMC Med Inform Decis Making.* [Online] 2015. https://pubmed.ncbi.nlm.nih.gov/26466787/

4. **Understanding Patient Data.** Understanding public expectations of the use of health and care data. [Online] 2019. https://understandingpatientdata.org.uk/sites/default/files/2019-07/Understanding%20public%20expectations%20of%20the%20use%20of%20health%20and%20care%20data.pdf

5. **The University of Manchester Centre for Social Ethics and Policy. In Partnership with the Patients association.** General Practice Data Trust (GPDT) Pilot Study: Report on Patient Focus Groups. [Online] 2023. https://www.patients-association.org.uk/blog/gpdt-pilot-study-report

6. **Information Commisioner's Office.** Personal data breaches: a guide. *For organisations.* [Online] [Cited: 19 May 2025.] https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/#whatisa

7. **NHS Digital.** Public attitudes to data in the NHS and social care. [Online] 2024. https://digital.nhs.uk/data-and-information/keeping-data-safe-and-benefitting-the-public/public-attitudes-to-data-in-the-nhs-and-social-care?utm_source=chatgpt.com#survey-findings

8. **Adminstrative Data Research UK.** A UK-wide public dialogue exploring what the public perceive as 'public good' use of data for research and statistics. [Online] 2022. https://www.adruk.org/fileadmin/uploads/adruk/Documents/PE_reports_and_documents/ADR_UK_OSR_Public_Dialogue_final_report_October_2022.pdf

9. **Data and Analytics Research Environments UK.** Building a trustworthy national data research infrastructure: A UK-wide public dialogue. [Online] 2022. https://zenodo.org/records/13869085

10. **Research Works, on behalf of Understanding Patient Data.** What words to use when talking about health data: Secure Data Environments and Trusted Research Environments. [Online] 2024.

https://understandingpatientdata.org.uk/sites/default/files/2024-05/WWTU%20Final%20Report_1.pdf

11. **Waind, E.** Trust, security and public interest: striking the balance. A narrative review of previous literature on public attitudes towards the sharing,linking and use of administrative data for research. *Int J Popul Data Science*. [Online] 2020. https://ijpds.org/article/view/1368/3116

12. **Information Commissioner's Office.** Understanding and Assessing Risk in Personal Data Breaches. [Online] 2023. https://ico.org.uk/for-organisations/advice-for-small-organisations/understanding-and-assessing-risk-in-personal-data-breaches/

13. **Godhwani, K., Saka, A.K., Ramasamy, V. et al.** Deliberative dialogue for co-design, co-implementation and co-evaluation of health-promoting interventions: a scoping review protocol. *Res Involv Engagem*. [Online] 2025. https://researchinvolvement.biomedcentral.com/articles/10.1186/s40900-025-00680-9

14. **NHS Health Research Authority.** Planning and Improving Research: Safeguards. [Online] 2018. https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/safeguards/#:~:text=Organisations%20must%20also%20have%20technical,for%20a%20purpose%20is%20processed

Appendices

I Participant demographics

A total of 50 participants registered for the initial workshops, with 47 attending. For the co-creation workshops a subset of 15 dialogue members were invited to participate. The aim was to recruit a variety of representatives from demographic categories of gender, ethnicity, age, socio-economic position, and residence across the four UK nations. Including a spectrum of health service usage was important as people's experiences with the health system may shape how they understand health data security. No other personal characteristics were collected, thus balancing the aim of representation of a variety of experiences with respect for the principle of data minimisation (14).

Participants voluntarily provided their demographics through a feedback form. Where data is missing due to participants choosing not to self-report, that frequency is included as 'blank'. For use of health service frequency (figure 3) and age bands (figure 5) participants were asked to select from pre-defined categories. The other demographics were generated from free text and grouped where appropriate. All collected participant demographics of the 47 dialogue participants are presented visually below, aside from the gender ratio which was female n= 25, male n= 20, non-binary n= 2.

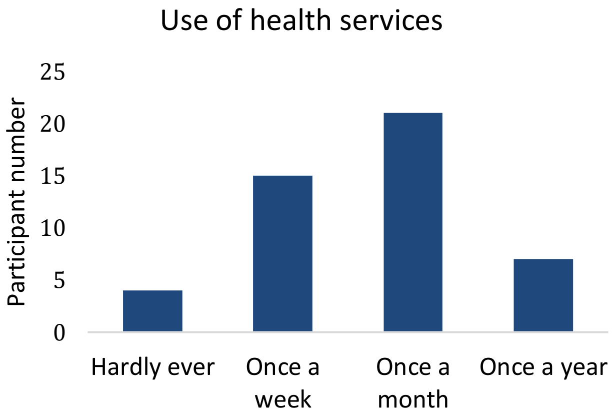


Figure 3: Approximate frequency of health services usage

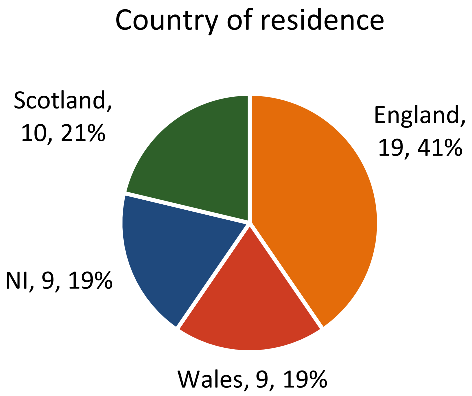


Figure 4: Current country of residence

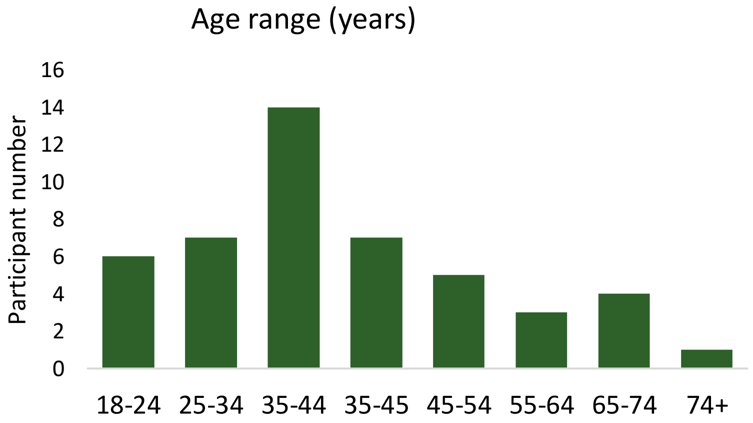


Figure 5: Participant age range collected in bands

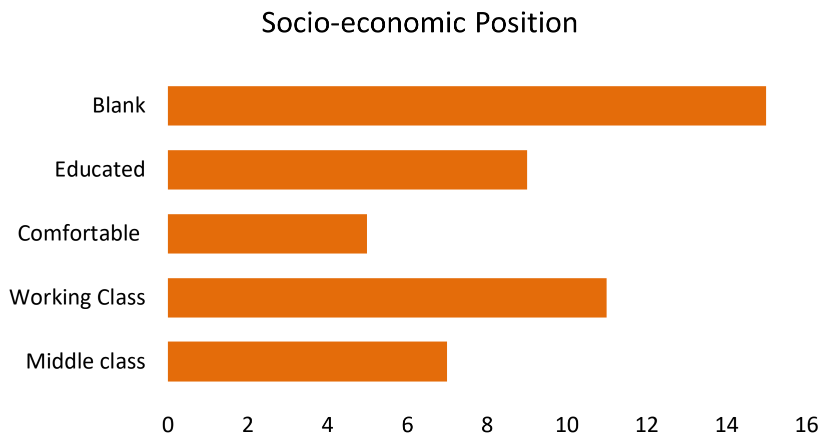


Figure 6: Free text socio-economic position (grouped)

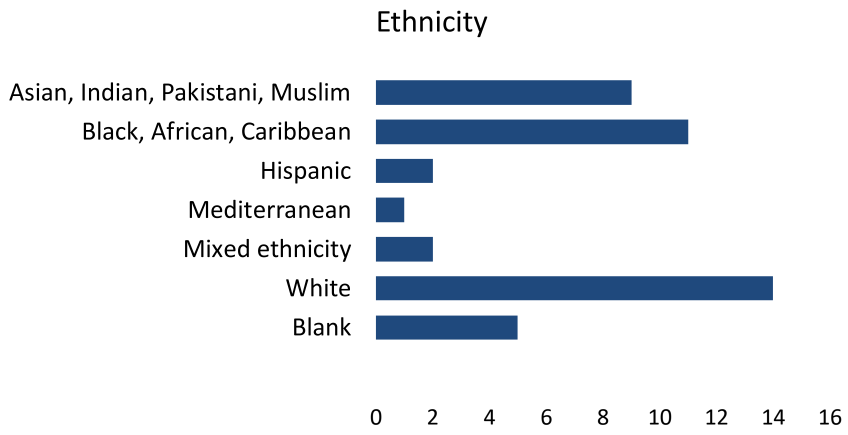


Figure 7: Free text ethnicity (grouped)

From this overall sample the co-creation workshops featured a sample of 15 participants with the following demographics. Categories have been collapsed.

Demographics of participants in the co-creation workshop		

Ethnicity
Mixed ethnicity = 2
White = 8
Black = 4
Asian = 2
	Country of residence
	England= 5
	NI= 3
	Scotland = 4
	Wales= 3
		Health service usage:
		Hardly ever= 4
		At least once a week= 0
		At least once a month= 8
		No more than once a year = 3

Gender
Male= 7
Female = 8
	Age
	34 or under= 6
	35- 64= 5
	65 or over= 4	

II Expert stakeholder interviews sample:

Invitations to participate were sent to a range of people across organisations and roles, identified in collaboration with UPD and with the project steering group members. Six experts agreed to be interviewed.

Expert Interview Sample:	
Stage	Roles/field
After 1st co-creation workshop	Head of Information Governance (IG) and Data Protection Officer
After 1st co-creation workshop	Head of Information Governance Policy Engagement
After 1st co-creation workshop	Self-employed Primary Care Information Governance Consultant & Former Data Protection Officer
After 2nd co-creation workshop	Data & AI Policy Manager
After 2nd co-creation workshop	Patient and Public Involvement and Engagement Manager
After 3rd co-creation workshop	Information Governance and Data Protection Lead